

User Registration and Login Methods

Using Alpha Five V8 Security Framework

Today, developers can choose among several different methods to allow users to register and gain access (login) to their Internet-based application. Although some are more popular than others, the method selected should be appropriate to the nature of the online application and the type of user expected, as well as provide for application security, data security and dynamic data filtering.

The purpose of this article is to review the most popular methods for online registration and login, the individual components of those methods, and to provide a general guide to web application developers incorporating user registration and login into their applications.

Programming examples are geared towards *Alpha Five version 8 deployed with the Security Framework*.

Because of this, you will see terms such as Security Framework, A5W and Ulink that refer directly to the Alpha Five development platform.

About the Author

Steve Wood has extensive experience building desktop and Internet-enabled software applications using Alpha Five. He formed AlphaToGo to serve a growing need for sophisticated desktop and Internet-based software applications for mid-sized companies. Steve is a Certified Alpha Software Solutions Provider, frequent contributor on the Alpha Message Forum and speaker at the annual Alpha Conference. See www.AlphaToGo.com for more information.

A special thanks to Chris Dickey for editing this document.

Copyright 2007, AlphaToGo – this document may only be reproduced if all pages are included along with copyright notice and footer information identifying the author.

User Registration and Login Methods

Using Alpha Five V8 Security Framework

Contents

About the Author	1
Background.....	3
Purpose of Registration and Login	3
User Registration requirements	3
User Login requirements	3
Examples of Registration and Login	4
Alpha Five	4
Why is Alpha Five used here?.....	4
Alpha Five Security Framework.....	4
Security Groups	5
Registration Components.....	5
Opt-In – Single or Double?	5
Login - Email Address or non-email value?	6
The Registration Form	6
Security Question	7
Captcha Validation	7
Assigning Users to Security Groups.....	7
Opt-out	8
Terms and Conditions / Privacy Policy	8
Registration Models	8
Open Model.....	8
Subscription Model	9
Authenticated Model	9
Methods for Established Companies.....	10
Login Models	10
Login Dialog	10
Lost password.....	10
Lost Username.....	11
Remember Me and Login Expiration.....	11
Recording Logins.....	11
Login using a Script.....	11
Deny user access	12
Conclusion	13

Background

Purpose of Registration and Login

Although scarce only a few years ago, it has become very normal for web sites and web applications¹ to have an option for visitors to log in. By doing so, the visitor is turned from just another “visitor” to a qualified “member.” As a member, they are offered access to additional resources, able to carry out secure financial transactions, or simply provided a more “rich and personalized experience.” Certainly, the impression is made that “logging in” somehow ensures each member’s information is safe and secure, and not shared with other members or the public.

It should come as no surprise that encouraging (or requiring) users to login is used to monitor the users’ online habits and predict behavior, especially purchasing behavior.

User Registration requirements

To be effective, four things have to take place during the registration process:

1. The user must provide credentials that uniquely identify them among all other existing members. This typically is an email address, or a non-email “username,” plus a password.
2. The online system has to properly deal with attempts by the user to register with credentials that have previously been registered. Responses range from simply denying the credentials provided, to suggesting alternate values or suggesting that the user is already registered and directing them to a page where they can log in.
3. In some cases, the online system must match the user who is trying to register with an existing customer database and only allow registration if the user provides information that positively identifies them as a member of this existing database.
4. Finally, the registration system must store the user’s login value along with other security information such that when the user logs in, the security system can positively isolate this user from other users, and display data and other resources that “belong” to this user.

User Login requirements

To be effective, five things have to take place when a user logs in:

1. The user must provide credentials that uniquely identify them among all other existing members. This typically is the user’s email address, or a non-email “username,” plus a password.
2. The login system must properly deal with incorrect username and/or password combinations. Responses range from simply rejecting the attempt to actually locking the user’s account after a number of attempts if the username was correct, but the password was incorrect.

¹ A *web application* is Internet-based software with a narrowly defined purpose, typically restricted to a specific group such as existing customers. A *web site* is generally available to the public.

3. The login system must positively match the values provided by the user with the database of existing user records – it has to ensure the person logging in, is the person represented in the user database.
4. In some cases, the system must provide for options which will automatically log that person back in when they return to the website.
5. Finally, the login system must provide options if the user has forgotten their login credentials, either username or password. These options almost always use a previously provided email address to transmit credentials, or require the user to answer a series of questions ensuring they are who they say they are.

Examples of Registration and Login

There are thousands of examples of web sites with the option to login, here are a few:

- *Social networking* web sites such as MySpace and LinkedIn where users develop a profile, share with others in an attempt to “connect” or accomplish some objective, such as finding a job or a mate.
- Your local utility company seeking to keep their customers well informed, while lowering the cost of preparing billing statements and collecting payment.
- Your neighborhood bank seeking to retain you as a valuable customer while lowering their cost by providing vital services in a manner convenient both to you *and* to them.
- A *somewhere far-away* business trying to capture you as a one time or repeat customer understanding that the Internet lowers the importance of their proximity to your location.
- And more and more today, the average small to medium-sized business trying to do exactly the same – lower cost, keep customers informed, take on more customers with less effort, and provide a more rewarding and efficient service that is convenient to both the customer and them.

Alpha Five

Why is Alpha Five used here?

Alpha Five is well suited to explain user registration and login models. Alpha Five is a software development platform that can be used to build very complex and highly functional desktop and Internet-based systems. At the same time, it is largely a point-and-click component-based environment making it more readily understood and even mastered, by non-programmers. For more information, see www.AlphaToGo.com or www.AlphaSoftware.com.

Alpha Five Security Framework

The Security Framework is new to version 8 of Alpha Five. If turned on, it virtually guarantees page and data security. It forces you to consider security at each level of your application and make a choice on whom can access data, how it is filtered, etc.

The Security Framework file system contains a very minimal amount of information, essentially just that necessary to allow or deny access and assign user rights. You cannot store extended information such as the user’s name and address. So, if you need those extra details you must include *a supplemental user table* as part of your system. This supplemental user table may be

1) built from scratch for this purpose, or 2) your company's existing User list (e.g. your list of Customers, Vendors, etc.). Your supplemental user table and the Security Framework need to be related on a unique key ID. In the Security Framework this key field is the Ulink ("User Link".) If you built your supplemental user table just for this purpose, the Ulink should be a sequential value that will increment with each new user. If you are using your company's own user list, it would be their established Account Number (or similar) assigned to the user based on their existing relationship.

Security Groups

An important aspect of the Security Framework is the concept of "Security Groups." Groups are used throughout Alpha Five to determine who has the ability to view, modify or delete particular elements of data, and control what resources are available such as menu choices, printing options, etc. As an example, your system may have the following Security Groups: Developer, Administrator, Customer, Vendor, Editor, Staff, Pending, and Restricted. Most systems have just two groups, an Administrator group, and one group for "everyone else."

Here are three examples of how you might use Security Groups:

- You may want to distinguish between members of your staff and Customers. Customers will likely have restricted access, relevant to them *as Customers*.
- If a new user decides to purchase your "Silver Subscription" they would naturally have access to fewer resources than if they had signed up for your "Gold Subscription." If they change their minds and pay your higher fee, part of your subscription payment process would change their Security Group from Silver to Gold and they immediately have access appropriate to that group.
- If your web application appeals to a particular industry or social group you may want to separate users by proficiency, such as Beginner, Intermediate and Advanced. Members would be able to view information appropriate to their respective group.

Registration Components

Opt-In – Single or Double?

Opt-In is the method by which the new online user "agrees" to register and join your service. Single opt-in is quicker, with only one step from sign-up to access. Double opt-in requires two steps and in the process ensures 1) the user really wants to register, 2) the user is who they say they are (they own the email account), and 3) they are less likely to claim that email from your domain is "spam." Double opt-in is preferred by those entities that monitor Internet spam and can restrict your ability to send email if complaints are received. If restricted, you may be asked to prove you have deployed a proper opt-in method.

Single Opt-In Process: Upon completing an online registration form, the user is 1) added to Security Framework with an appropriate security group, 2) immediately allowed to log in, and 3) sent an email with login details as a reminder.

Double Opt-In Process: Upon completing an online registration form the user is 1) sent a "confirmation email," 2) added to the Security Framework assigned to a security group named Pending and 3) added to your supplemental user table, if applicable. They must receive this

email and click an embedded link in order to “confirm” their intent to register for the service. Using Alpha Five, the link would lead to an A5W page that changes their security group from Pending to User (or whatever you designate), and they are allowed to log in. An email is sent to their address with login details as a reminder. If they do not respond, you may choose to delete their Pending registration after some period of time.

If they attempt to log in without first responding to the confirmation email, you may redirect them to a page repeating the instructions regarding the confirmation email. A link on this page should also allow them to re-send a new confirmation email. This method is only possible if you added them to the Security Framework when they registered. That is, if a user does not have a record in the Security Framework, all you can do is deny access.

Login - Email Address or non-email value?

Both Email Address and a non-email value are acceptable as the login credential. An email address is easier for the user to remember, and definitely unique to that user. A non-email value allows a bit more flexibility in that the login parameters stay the same even if they change their email address, perhaps due to a change in employment. Using email address is also less secure in that the persons email address can be determined, leaving only the password as an unknown.

Often, the user has an existing relationship with the online provider so an “Account Number” is used as their login. But this is not advisable because the user will not likely remember their Account Number on demand.

Here are the important factors: 1) the system must ensure the login value are unique*, 2) the system should not switch methods once in use, 3) in most cases the login values should be created by the user (not by you), and 4) internally the system should associate the login value with an sequential ID or an existing Account Number. The last one is explained under Alpha Five Security Framework above.

* The login value will always be forced unique within the Security Framework.

The Registration Form

The registration form is where your user signs-up for your service, providing username, password, etc.

One stage - ask for all information necessary on the first page. Useful only if user is strongly compelled to register.

Two or multi stage – ask for the least amount of information to encourage sign-up. The bare minimum would be username and password. Ask for additional information on subsequent page(s), or when user first logs in, or passively in their “MyProfile” page. This is useful if it is likely that the user will abort the registration process if asked for too much personal information. If they do not complete the rest of the application you can, if appropriate, use the email address you gathered on page one to remind them to complete the registration or to offer additional services. Multi-stage registration forms are far more common than single stage.

Security Question

Another option is to require the user to pre-answer a “security question” such as “what is the name of your first pet.” The question and the answer are stored as part of the user record in the Security Framework. Later, if the user forgets their password, they can be required to re-answer this question in addition to providing the email address you have on file. This is a standard feature of the Security Framework.

Captcha Validation

This is a fairly new technology designed to ensure the “person” registering or trying to access resources is, in fact, a human being and not a computer program. It is normally presented on the same page requesting username and password. The most common use is to present a difficult-to-read graphic with letters and numbers, and require the user to re-type those values. The system will then compare the two values, and if they match, the user will be allowed to proceed. Another method is to present a simple math problem to the user, such as $2 + 4 = ?$. Both of these can be created in Alpha Five.

Assigning Users to Security Groups

You may want to categorize users on your system, for instance, to provide different rights to Customers and Vendors. You can either assign them into Security Groups when they first register, or manage the user list after the fact (or both.) This can get problematic, so it’s best to keep it simple. Examples:

- Include a required field on your registration form such as “Access Code.” Send an email to all of your Customers and Vendors. Tell your customers to enter “CUSTOMER123”, and tell your Vendors to enter “VENDOR987.” During registration, capture this value and assign them to the appropriate Security Group. This method is not without complications, not least being they forget the Access Code and call you when they are denied registration.
- Same as above, but the “Access Code” is embedded in a URL link included in the email. The link leads to a processing page that registers them and automatically puts them in the appropriate security group. The URL might look like this www.mydomain.com/myreg.a5w?secgrp=cust&fn=Steve&ln=Wood. With that information you could say “Hi Steve Wood” and, when they complete the registration, put them in the Customer group.
- If you have an existing customer list you can pre-determine which security group they will be assigned to once they register. Anyone not on this existing list may be assigned to a standard group or perhaps denied access.
- In some cases it may be useful to let users to determine what group(s) they want to belong to. For example, if your website provided advice to Golfers, users might choose between Beginner, Intermediate or Advanced. This of course, is not really a “security” implementation and there are other methods to accomplish the same thing.
- Of course you can just add all of the users yourself with each person in the appropriate group. I.e.: no one registers, you do it for them.

You can manage the live User’s list in one of three ways:

- Use the Alpha Five feature under Web Security > Options to import the users from the website to the desktop, make changes, and then publish that list back to the website using Web Security > Publish Security Files (and check the Users and Groups box.) This is only advisable where you do not expect anyone to log in or register between the time you import, adjust and then upload the modified user list.
- Design your own system to manage Users completely online.
- You can purchase third-party web templates that include user management. See www.AlphaToGo.com for several such packages.

Opt-out

You must provide users with a method to unsubscribe or “opt-out” from your service. Check the bottom of any commercial email to see how this is displayed. Your unsubscribe link can lead to an A5W page that takes their information (normally as a URL parameter) and removes or “inactivates” their record. It is becoming popular to offer the user some “subscription choices”, to ask questions why they are unsubscribing, and to gently nudge them to maintain their subscription.

The ability to opt-out should be on every email and available while logged in. If they request to be removed, you should remove them from the Security Framework and if used, from your supplemental user table.

Terms and Conditions / Privacy Policy

Don’t over-look these. Your prospective online user must agree to a particular set of Terms and Conditions and/or Privacy Policy when registering for your online service. This is for your own legal protection, and provides full disclosure to the prospective member. There are plenty of examples of these documents on the web.

Registration Models

Open Model

Examples: Yahoo!, LinkedIn, Amazon, where anyone can register and you are a member – “forever.”

Users self-register and have no pre-existing business account.

Registration process example: Steve registers online with Username: steve123 / Password: bianchi. He passes successfully through your opt-in process and you write a record to your supplemental user table. The table is set to auto-increment an ID value, and it comes back with “00000010.” You then write a record to the Security Framework with “00000010” as the Ulink, along with the username, password, and security group information. Based on Terms & Conditions you presented to the user during registration, routine emails may be sent to remind Steve of your services, etc.

Login process example: When Steve logs in as Steve123, the Security Framework grants access and places “00000010” into a session variable. The session variable plus security group

information is used as a filter to ensure Steve is only able to view information appropriate to him.

The supplemental user table record might look like this:

Ulink	Name	Address	LastLogin
00000010	Steve Wood	250 First St.	10/10/2007

Subscription Model

Examples: Consumer Reports, MotleyFool, Wall Street Journal.

Users self-register, have no existing business account, and access is based on current subscription status.

Registration process example: Steve registers online with Username: steve123 / Password: bianchi. You initiate your opt-in process and write a record to your supplemental user table. The table is set to auto-increment an ID value, and it comes back with “00000010.” You then write a record to the Security Framework with “00000010” as the Ulink, along with the username, password, and security group information. At this stage, the user has not completed the subscription payment process, so they will be assigned to a security group named Pending. Based on Terms & Conditions you presented to the user during registration, routine emails may be sent to remind Steve of your services – and they haven’t even paid yet!

Payment process example: Simultaneous with the opt-in process, you pass Steve’s information and the “00000010” ID to the payment gateway as a POST transmission. The user either does or does not complete the payment process, resulting in a success or failure notice from the payment gateway. The response comes as a POST to a particular URL on your system, along the user’s ID. The URL might look like this:
www.mydomain.com/pmtproc.a5w?id=00000010&status=success. The response is normally immediate, but could be many hours later. If it returns a success, you use the ID provided to move that person from the Pending security group to a normal group. The new user’s record is noted with the subscription expiration date, if applicable.

As the expiration date nears, the subscription is either automatically renewed or an email is sent asking the user to re-subscribe. If subscription is not renewed, the user’s record is still retained and may be used to encourage the user to “come back”.

There are many variations on the above depending largely on how you process the payment.

Login process example: When Steve logs in as Steve123, the Security Framework grants access and puts “00000010” into a session variable. That session variable is used as a filter to ensure Steve is only able to view information appropriate to him.

The supplemental user table record might look like this:

Ulink	Name	Address	LastLogin	Expires
00000010	Steve Wood	250 First St.	10/10/2007	10/1/2008

Authenticated Model

Examples: Your bank or local utility company where you have an existing account.

Users self-register but have to be matched to an existing customer list.

Registration process example: Steve registers online with Username: steve123 / Password: bianchi. During registration, you ask Steve to enter his Account Number and other details for authentication (things only Steve would know.) If you validate that Steve is the rightful owner of this account, he passes through your opt-in process and you write a record to the Security Framework, copying his Account Number to the Ulink field.

It's entirely appropriate to "lock the users account" for some period of time if someone fails three to five times to gain access with a given Account Number. You would want to contact the account holder if possible in that case. This is a standard option of the Security Framework.

Login process example: When Steve logs in as Steve123, Security Framework grants access, and puts the Ulink value (their Account Number) in to a session variable. Same as above, that variable is used as a filter to determine what information is available and is included in any new data saved during the session.

Your user list record might look like this:

AccountNo	Name	BillCloseDate	LastLogin
AB3-R123	Steve Wood	2	10/10/2007

Methods for Established Companies

Many established companies want to "go online" and move some or all of their customers from traditional communications methods to an Internet model. Here are two useful methods for this:

- Use your existing Customer list, get everyone's email address, pre-assign everyone a login and temporary password, import that into the Security Framework, and send an invitation to the entire list, asking them to sign in. Watch for who does/does not sign in, and remind them with emails as appropriate.
- Same as above, but do not pre-establish your list. Just ask everyone to go to the website and create an account. If you have an existing Customer list, use the Authenticated Model for user registrations.

Login Models

Login Dialog

There is significantly less to say about Login models given they almost always have the same appearance, a simple request for username and password. The username can be either the user's email address or a non-email value. On rare occasion the username is an "Account Number" or other value not created by the user.

Lost password

Most systems provide users with the ability to recover a lost password. The system will allow the user to either 1) recover the existing password or 2) reset the password to a new value. In either case, the password is typically sent via email to the "email address on file" (provided

during registration.) If the user has changed their email address, the system may offer additional options to recover the password such as displaying it on-screen, or sending the password to a newly provided email address. In all cases it is mandatory that they system ensure the user prove they are the owner of the account, and should receive the password. If you use the Security Framework properly, the password is never known to anyone but the appropriate user.

It is not appropriate for the user to be able to call your Customer Service center to retrieve their password. No one should ever know the password other than the user. Your password recovery system should be the only way a user can recover their password. However, Customer Service should be able to *reset* the password to a new value, and your system should then force the user to change that password when they first log in.

It is also not wise to send both the username and the password in the same email. This may seem insignificant, but this slight inconvenience will ensure no single document provides all values required to login.

Finally, it is less secure to display on the login page, that the user provided a valid username, but the password was incorrect (or vice versa.) Do not provide the user/hacker with any such “assistance” in their attempt to log in.

Lost Username

It is less common to be able to recover a lost username value. Often, the user is required to call the company and prove their identity to have this information provided to them. However, Alpha Five provides this option, requiring the user to provide a valid email address and/or answer other security questions.

Remember Me and Login Expiration

You can use the Security Framework to determine when a login expires. Some of the options are 1) immediately when the user closes the browser, 2) a specified amount of time (either from initial login or the amount of idle time), or 3) based on web server settings. You can also render the user perpetually logged in using the “Remember Me” option. The Remember Me (and other options) places a cookie on the user’s computer containing login credentials and expiration information.

Web applications containing financial and other private information should never deploy any automatic login features.

Recording Logins

It is useful to monitor login, logout and other activity on your web application in order to gauge performance and effectiveness. The Security Framework can be set to keep a basic log all successful logins. However this record list is quite limited, including only login date and time, user identification and login expiration date. If desired, it is easy to add a more complete log of user activity including page access, page duration, successful and failed login attempts.

Login using a Script

Some systems offer functions to automatically log a person in via a script. In this case, a URL could include parameters that automatically log someone in. This should be approached with

extreme caution and is not acceptable for the average web application. An acceptable situation might be to perform automatic log in with a security group with absolute minimal access rights, to perform some maintenance process, and then automatically log out.

Deny user access

You can deny access in one of three ways:

- Use the Security Framework “Lockout” function to temporarily deny access to a user. When they attempt to log in a message customizable message will simply say they are temporarily denied access. The lockout feature is not designed for restricting a user indefinitely.
- Manually change the user’s password, so they are unable to log in. This is an quick and easy fix, but is not designed for restricting a user indefinitely.
- Assign them to a Security Framework Group such as DenyAccess. When they attempt to log in, that assignment can redirect them to a page explaining their options.
- You can leave their Security Framework record intact but block access with a field in your supplemental user table such as “DenyAccess.” Set this to True, and write the appropriate code to deny access. This might be applicable if you have a variety of “reasons” for lockout, give them restricted access, or want to capture login attempts, etc.
- You could, of course, just delete their login record.

Note: short of IP restriction, if you use any of the open methods above, you can never absolutely prohibit a user from signing up again and creating a brand new account.

Conclusion

This article discussed various methods and models for user login and registration. Based on my own experience, I used Alpha Five Version 8 for all programming methods. I hope by writing in terms of “process” instead of “software code” I have made this article readable by non-programmer business professionals as well as both beginning and accomplished developers.

Many related subjects have been omitted from this article – web site security, encryption, SSL, database choices, and additional features of Alpha Five and the Security Framework. I also left out any of the actual code you might have to write in order to put these methods to work.

I saved one more topic for the conclusion, and that is Responsibility. If you represent a large bank, medical or financial institution, how you protect user information is regulated by several laws. However, as a small or medium sized business, you are likely not covered by these laws. In the process of building a web application, you will open your server to the world wide web, and the truth is, this is not a friendly environment. Assume (because it is true) that attempts will be made to hack in to your system. It is your awesome responsibility as a developer and/or business owner to protect your user’s private information. If you are not adept with LAN and Internet security, you might find someone to at least review your hardware and software configuration. Take the time to understand basic security – protect your web server, LAN and database from both Internet-based and internal company threats. Respect your user’s privacy.

If you are not an Alpha Five user and would like more information, we encourage you to visit Alpha Software at www.AlphaSoftware.com or see our website at www.AlphaToGo.com.

Any comments or questions regarding this article should be directed to steve@alphatogo.com.