SeniorSystems

Advantage Cloud Two-Factor Security Process

Advantage Cloud Two-Factor Security Process

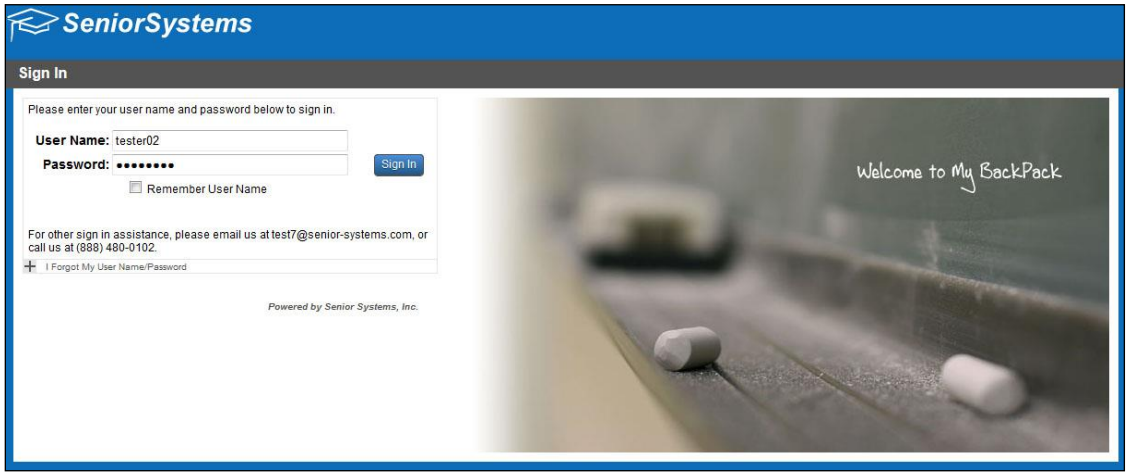
Table of Contents:

1. Why use Two-Factor Authentication?

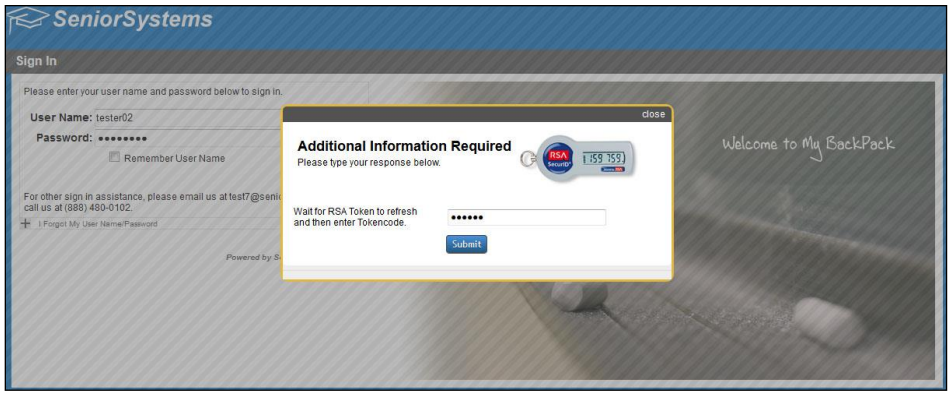
Two-Factor Authentication provides your school with a second level of enhanced security to greatly reduce the risk of security threats. Two-factor authentication offers a security process in which the user provides two means of identification, one of which is an RSA security hardware token. This RSA security token generates a secure 6-digit Tokencode in 60-second intervals. The other security factor is your My BackPack Username and Password. Invoking a Two-Factor Authentication plan is the perfect way to protect your school's sensitive data.

When Two-Factor Authentication is activated for your school, any LDAP users who have been set up to use Two-Factor Authentication will first be prompted to enter their My BackPack Username and Password. They will then be prompted to enter their RSA Tokencode that is generated from their RSA token hardware. It is best practice to wait for the next Tokencode to regenerate, before entering the Tokencode.

My BackPack Login screen:



RSA Token and My BackPack Tokencode Login screen:



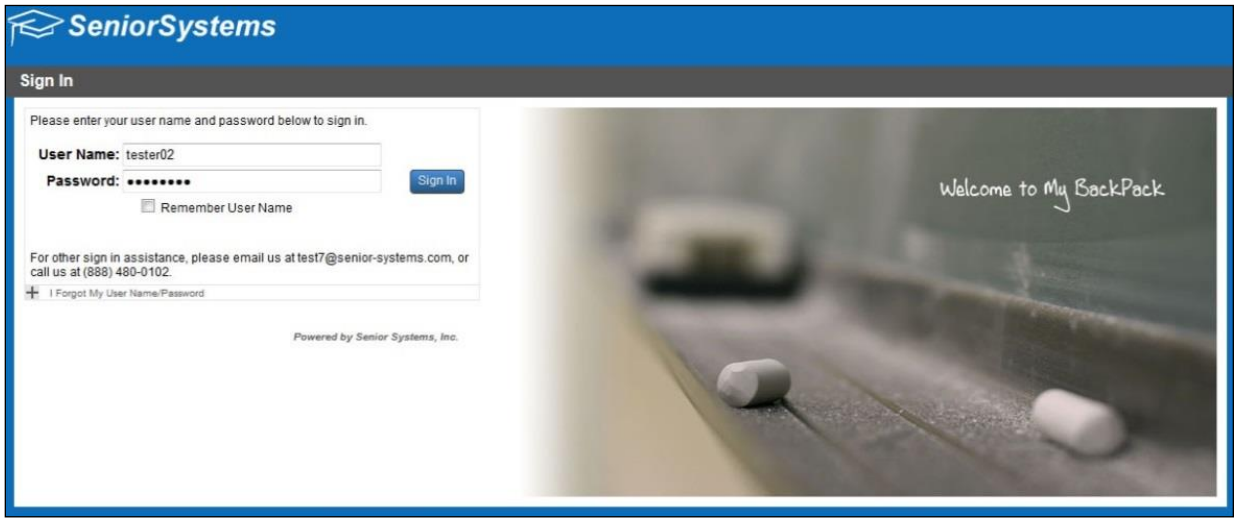
2. Two-Factor Authentication Guide for Faculty Members

Hello and welcome to the Two-Factor Authentication Guide for Faculty Members!

This Guide describes how to use your new RSA Token to securely access My BackPack. The RSA Hardware Token that you have received generates a new 6-digit password every minute. To access My BackPack with your RSA Token, you will first need to access the My BackPack website and enter your normal Username and Password. You will then be prompted to enter the RSA Tokencode displayed on your RSA Token.

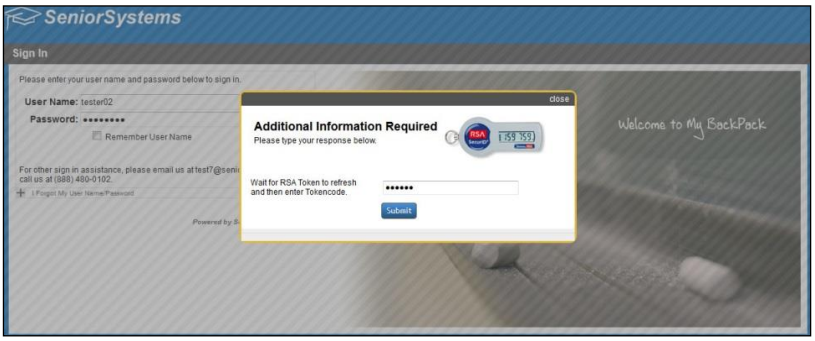
Accessing My BackPack with the Two-Factor Authentication process:

1. Open your preferred web browser, and enter the My BackPack URL in the address bar.



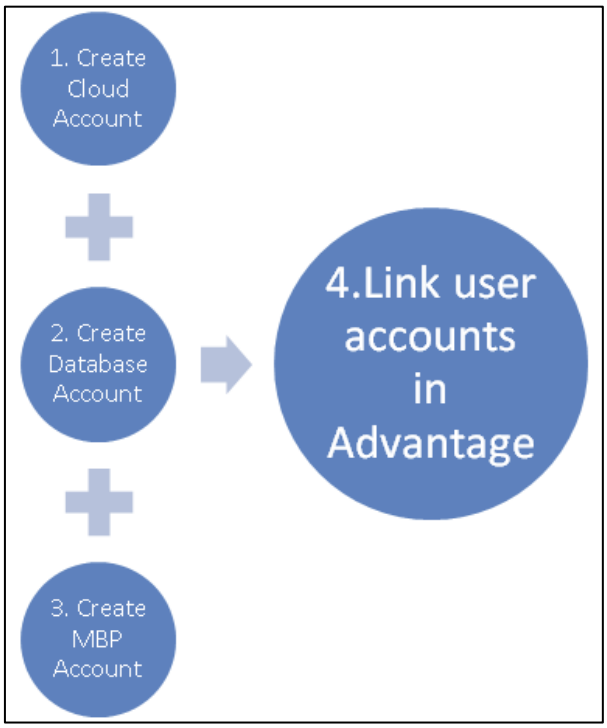
2. Enter your Username and Password in the appropriate fields and then click **Sign in**.

3. You are now prompted to enter your RSA Tokencode. Wait for the RSA Tokencode to refresh and then enter the Tokencode.



3. Setting up User Accounts with Cloud Authentication

An individual will need a Senior-Anywhere (Citrix) user account, an Advantage user account and a My BackPack user account to enable Cloud Authentication. The setup process essentially associates the three accounts, so that the individual can access Senior-Anywhere (Citrix), Advantage and My BackPack with a single set of credentials. Once these three have been created and linked, and the RSA Two-Factor Authentication preference has been enabled, all LDAP users will be required to enter their RSA Tokencode when they attempt to log into My BackPack.

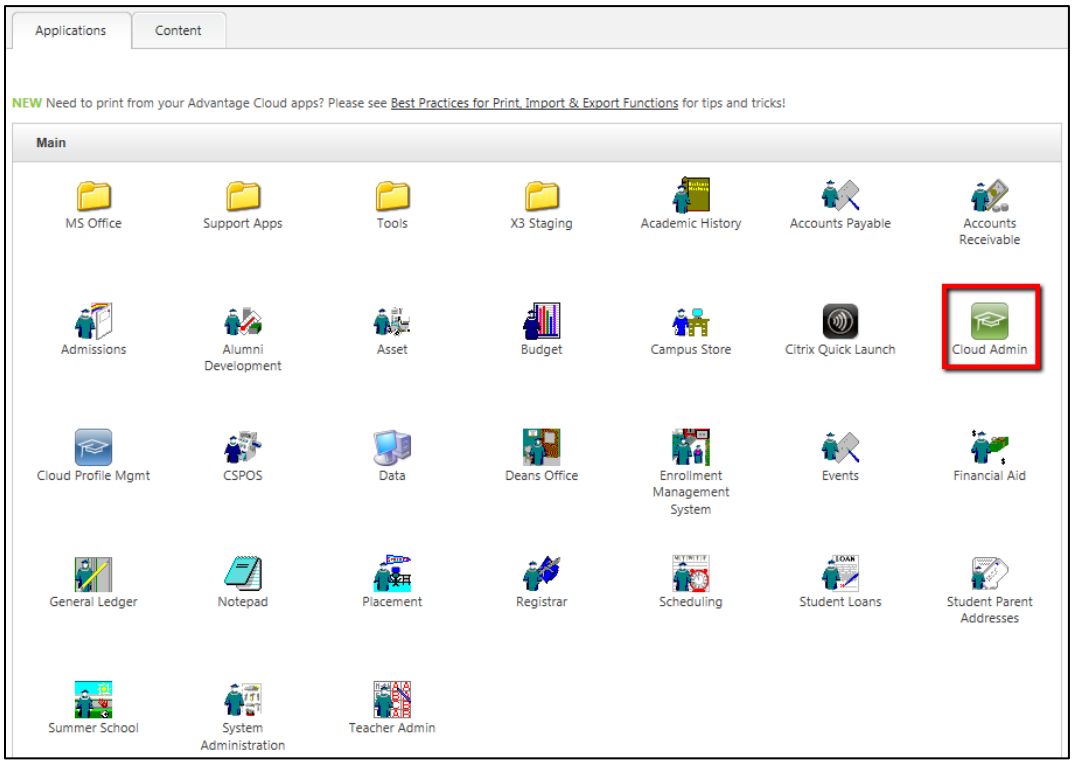


Contents:

Part 1: Creating a Senior-Anywhere (Citrix) User Account

1. Open your preferred web browser and log into https://www.senior-anywhere.com with a user account that has CloudAdmin permissions.

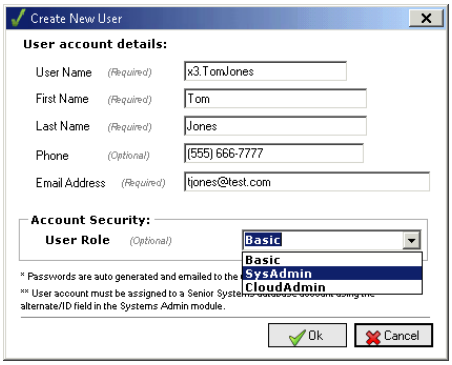
2. Once you have logged in, double-click the **Cloud Admin** icon.



3. Click the **Add** button to add a new Cloud User Account.

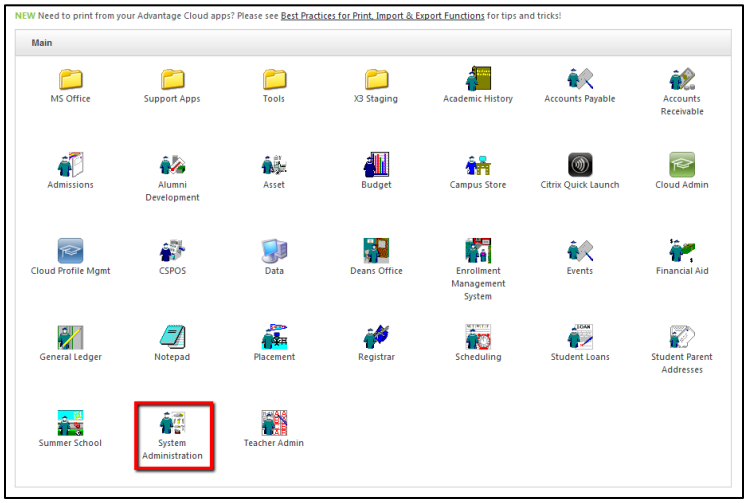
4. Enter the necessary information in the Create New User screen, including the user's email address and the appropriate User Role, and click **OK**.

NOTE: The email address that is entered will receive an email containing a temporary password, which will need to be changed to a real password during the user's first login attempt.

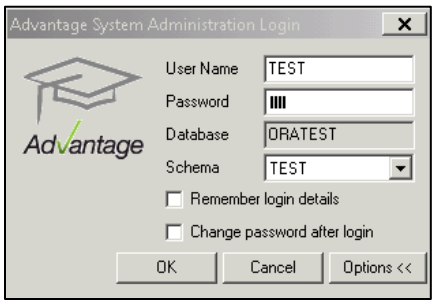


Part 2: Creating an Advantage User Account with Cloud Authentication

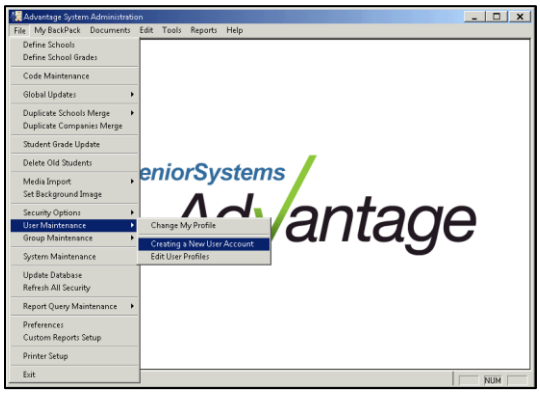
1. After you have created Faculty Member Senior-Anywhere Cloud User Accounts, you can now create Faculty Member Advantage Database User Accounts. Open the System Administration application.



2. Enter the User Name and Password of the schema owner and click **OK**.

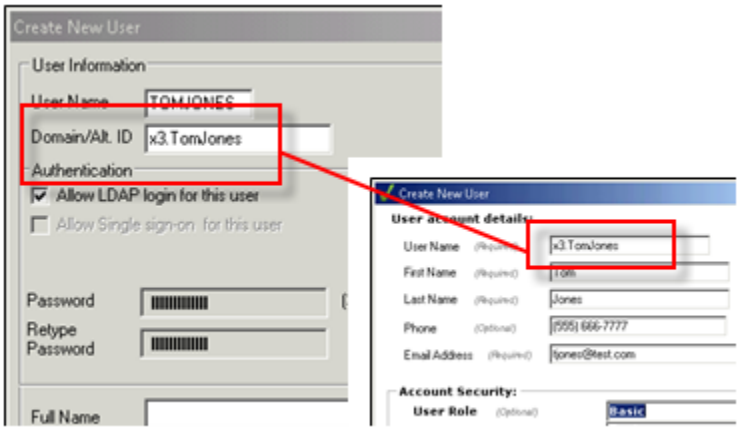


3. Click **File** > **User Maintenance** > **Creating a New User Account**.

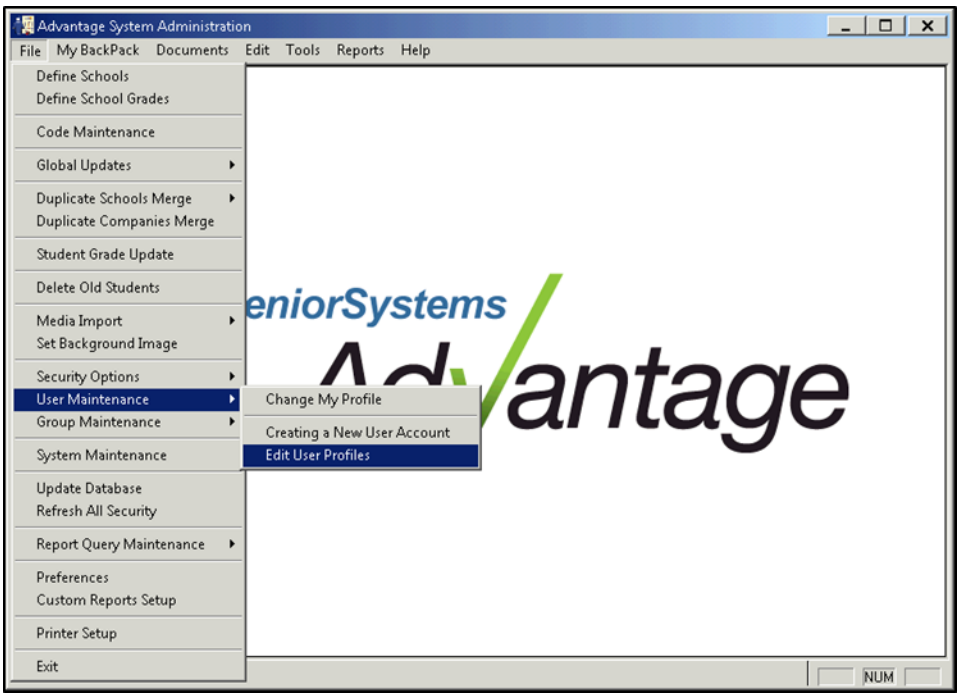


4. Enter a **User Name**, **Domain/Alt. ID**, and click the **Allow LDAP login for this user** checkbox. Click **OK**.

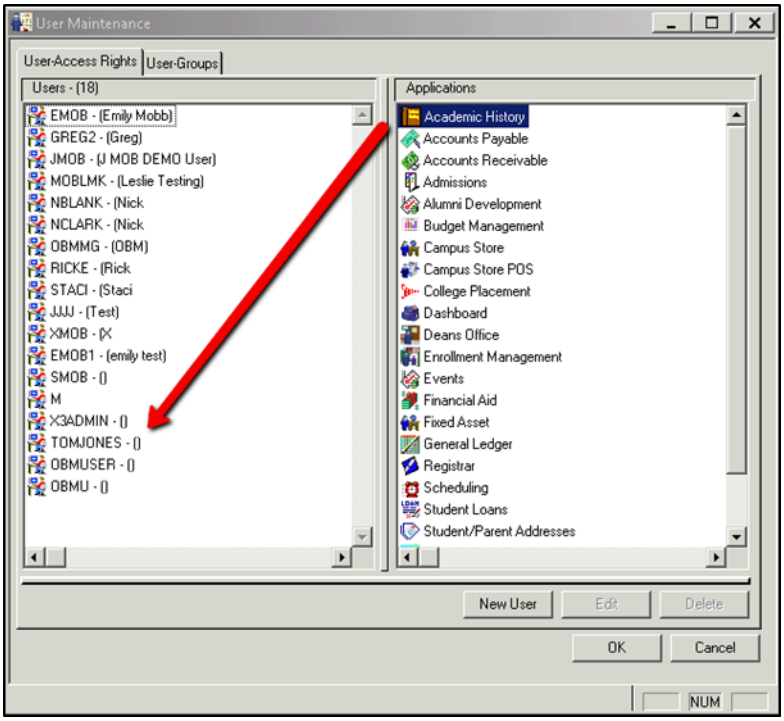
NOTE: In the **Domain/Alt. ID** field, you must enter the UserID of the Faculty Member that you entered when creating the Cloud Account. For instance, in the example provided in these instructions, you would enter **x3.TomJones**. If you have forgotten what you entered for a UserID, you can open the CloudAdmin tool and locate the UserID that you have entered previously.



5. Click **File** > **User Maintenance** > **Edit User Profile**.

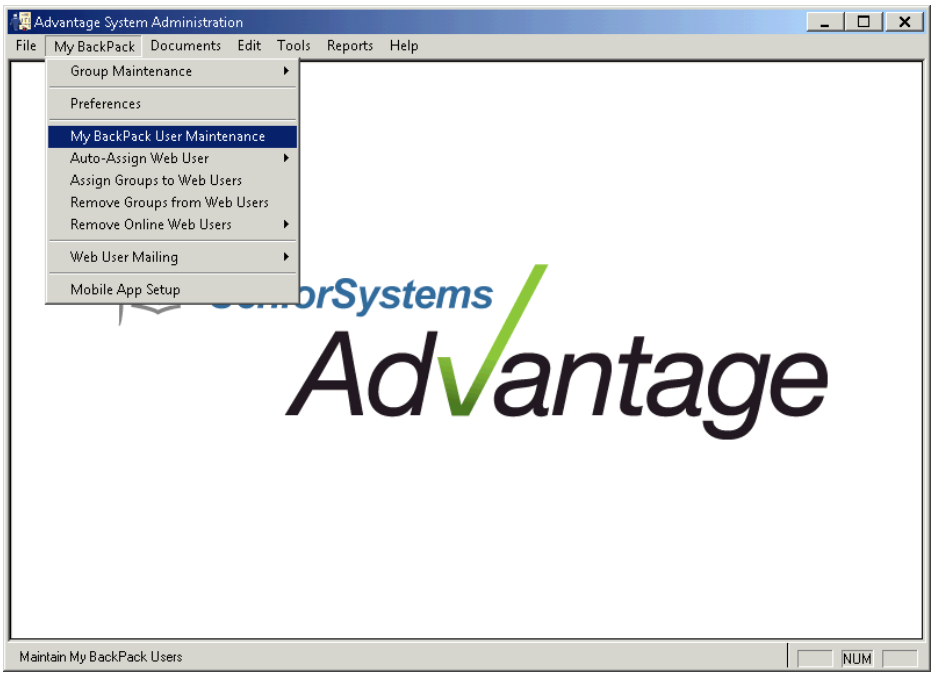


6. Drag and drop the applications to which the user needs access permissions and click **OK**.

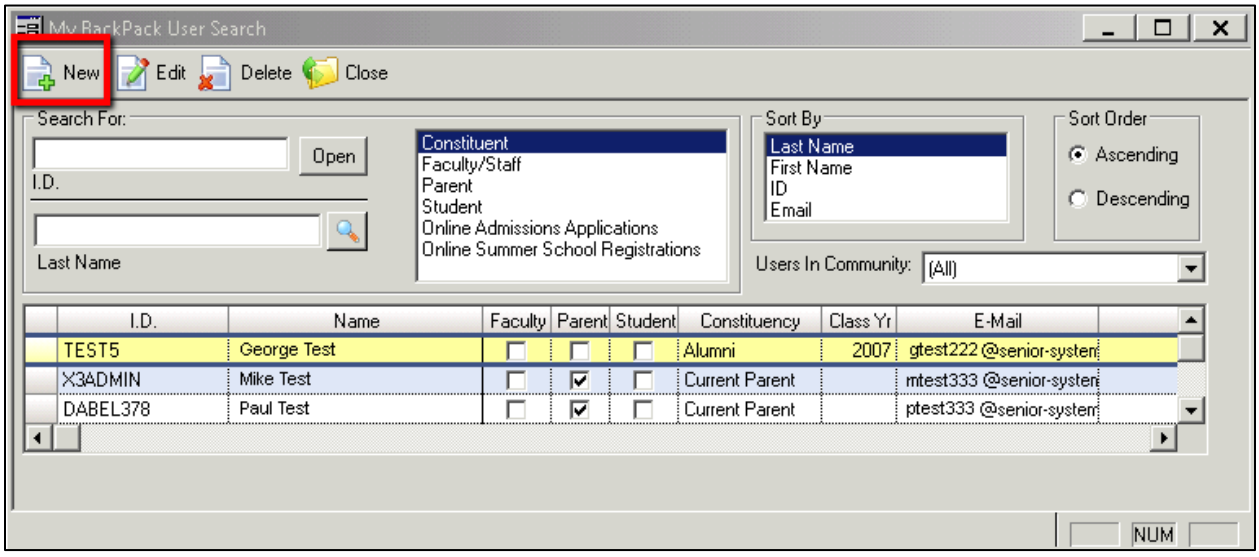


Part 3: Creating a My Backpack User Account with Cloud Authentication

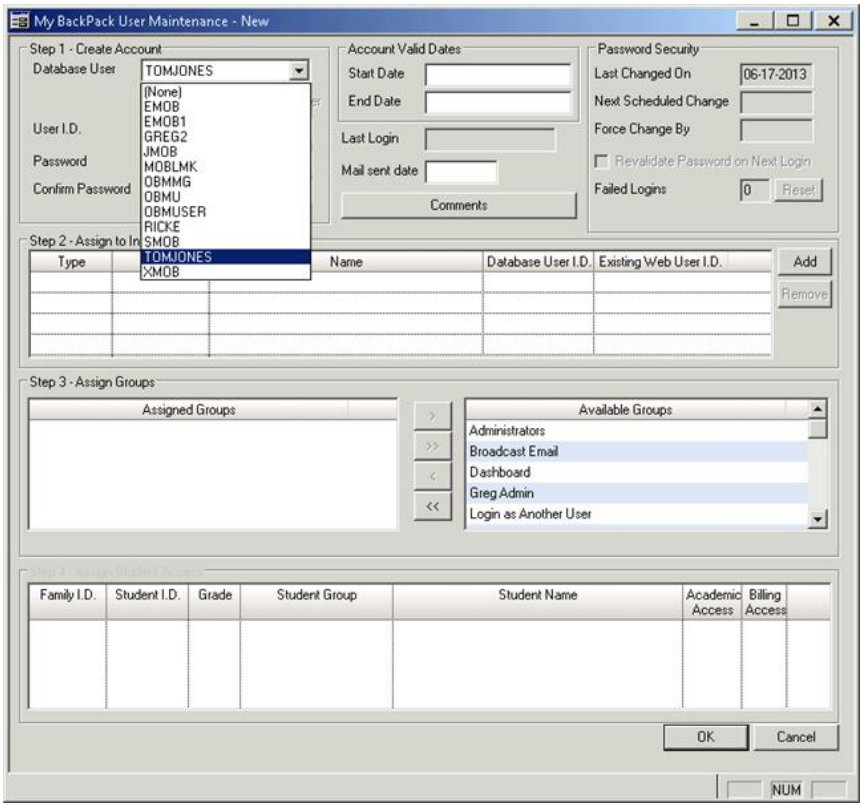
1. Once you have created an Advantage User Account with LDAP Permissions, you will now want to create a My BackPack user with LDAP permissions. Click **My BackPack** > **My BackPack User Maintenance**.



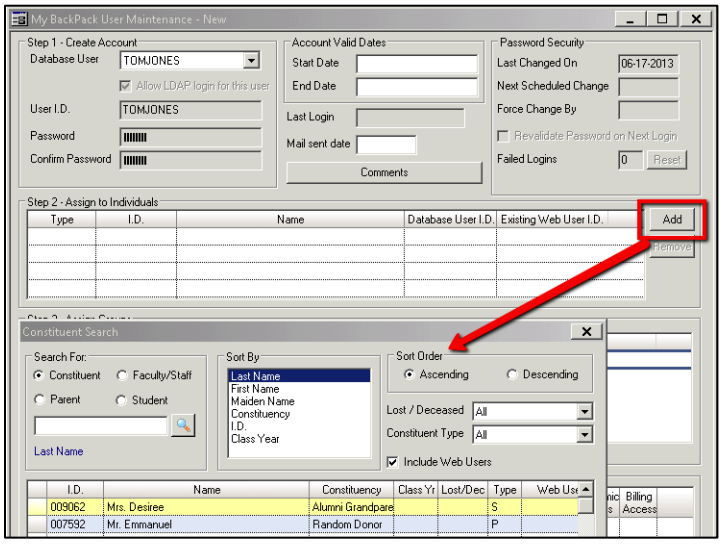
2. On the My BackPack User Search screen, click **New**.



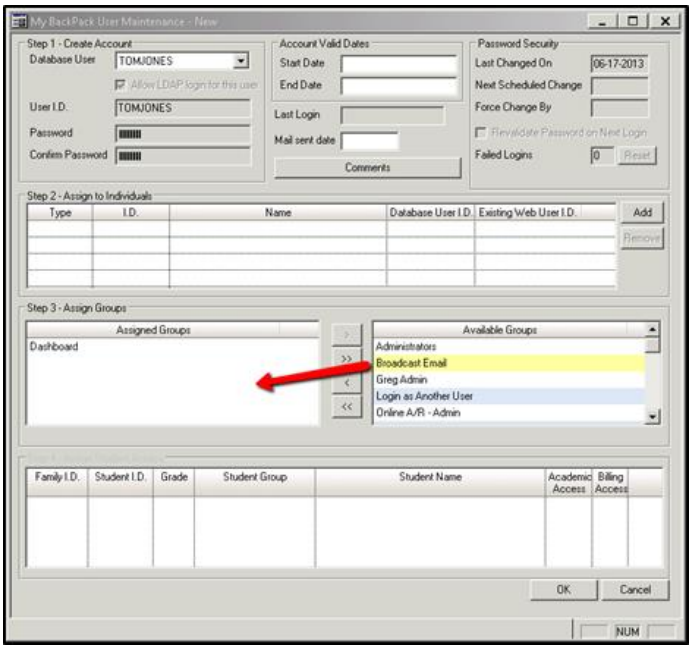
3. Select the Database User that you created from the **Database User** drop-down menu.



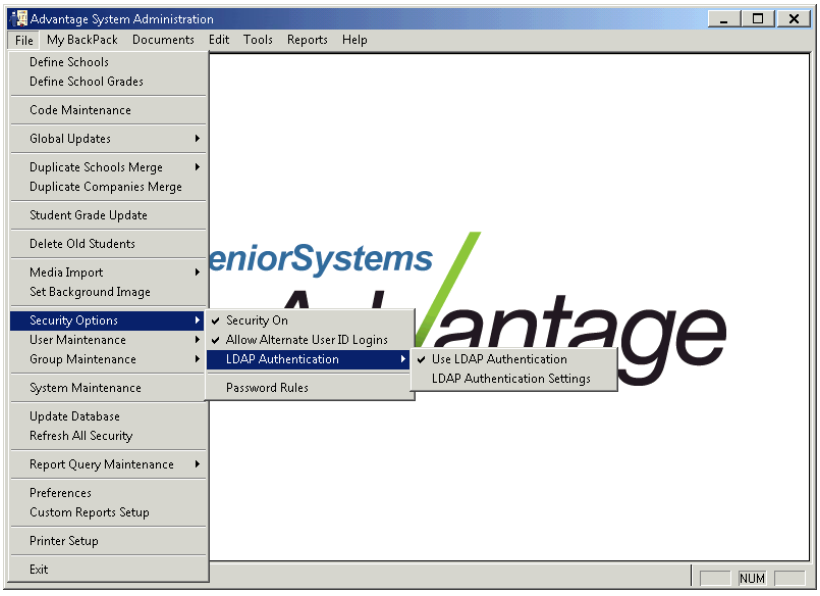
4. In the **Step 2 – Assign to Individuals** area, click **Add** and assign an individual to the My BackPack user that you are creating.



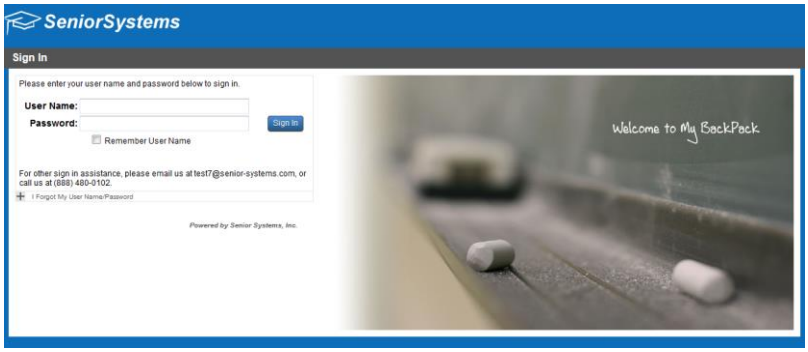
5. Assign groups to the user that you are creating by dragging groups from the **Available Groups** area to the **Assigned Groups** area. Click **OK**.



NOTE: Now that you have successfully created a My BackPack User, you need to ensure that the security options are set up correctly. Click **File** > **Security Options** > **LDAP Authentication** and check **Use LDAP Authentication**. Also ensure that **Security On** and **Allow Alternate User ID Logins** are checked.



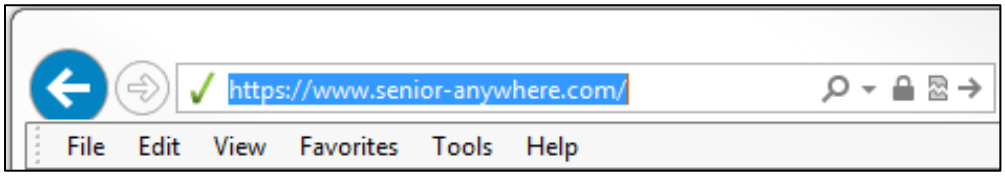
6. Now you will be able to log into My BackPack with your Cloud Account Username and Password.



Part 4: Logging into the https://www.senior-anywhere.com/ website

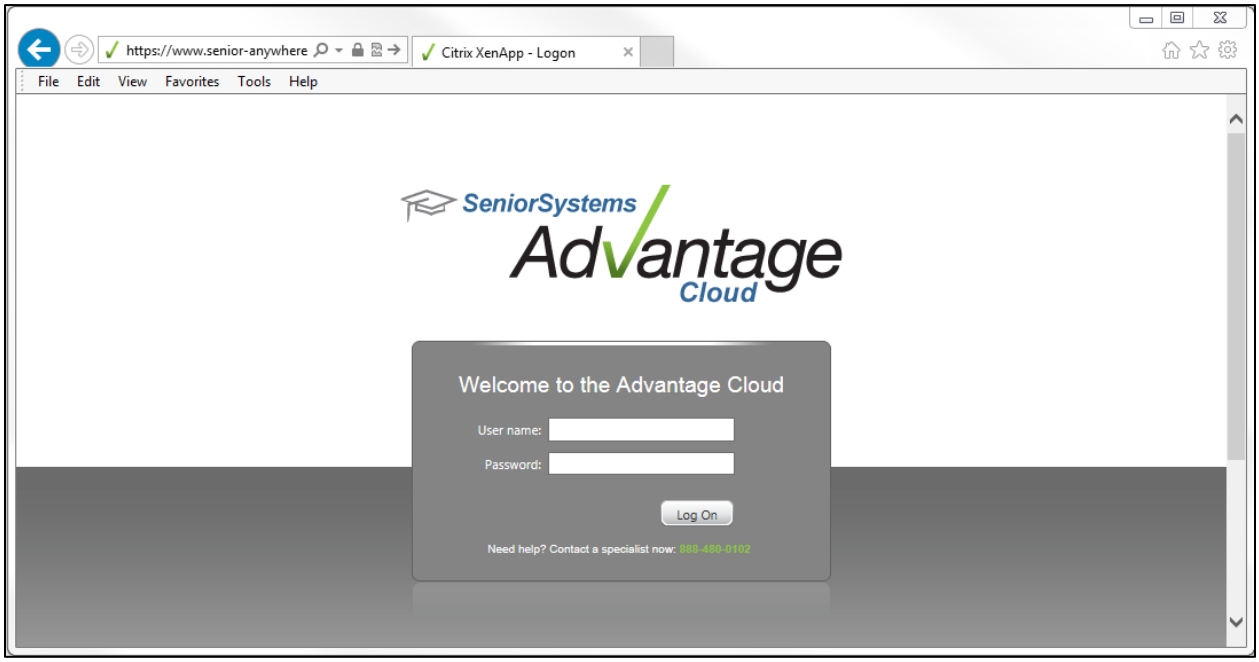
1. Open your preferred web browser and enter the following URL into the web address bar:

https://www.senior-anywhere.com/

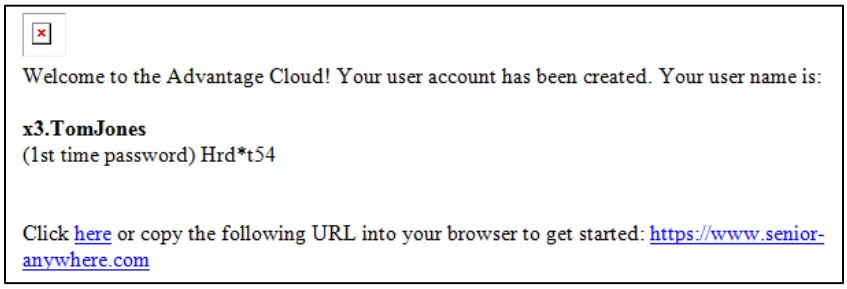


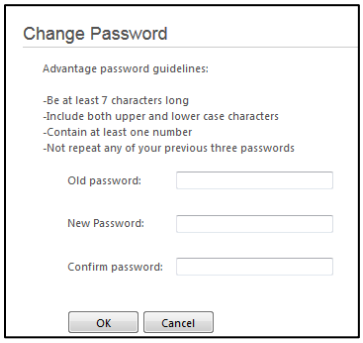
2. After you enter the URL into the web address bar of your web browser, and press **Enter**, you may be prompted to install the Citrix Receiver. If necessary, install the Citrix Receiver, then come back to this page, and continue following the login instructions from this point.

If you are not prompted to install the Citrix Receiver, you will see the following login screen:

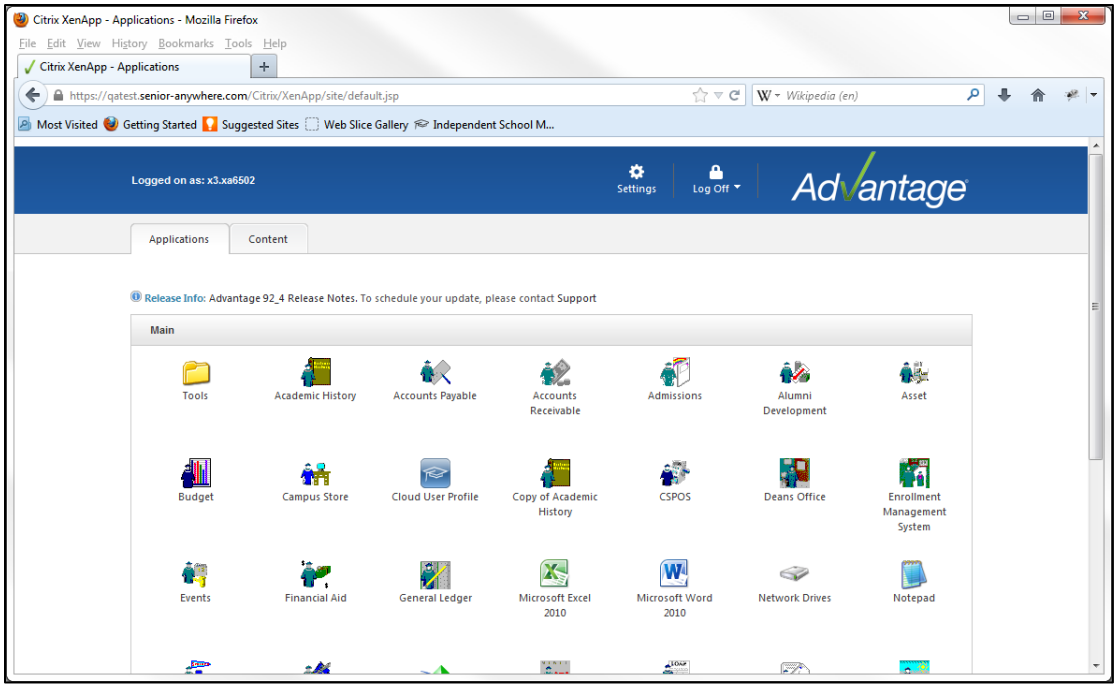


3. In the Cloud Login screen, enter the Username and temporary Password that were sent to you via email. You will then be prompted to change your temporary password to a real password. Click **OK** once you have entered your real password twice.



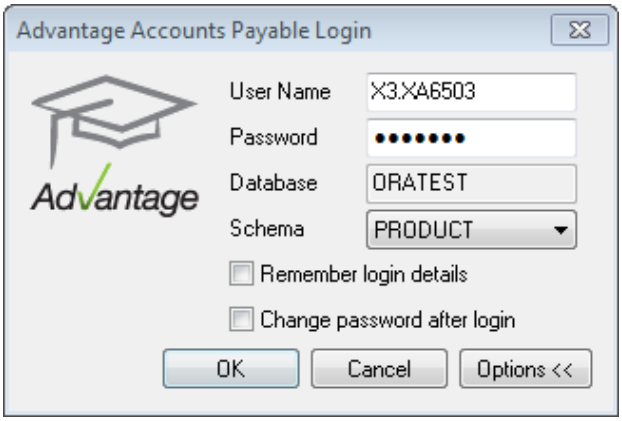


4. Once you are logged into the https://www.senior-anywhere.com/ website, you will see the following homepage.



5. Click the application that you would like to work with in the Cloud environment. When the Login screen appears, enter your Username, Password and select the schema from the drop-down menu.

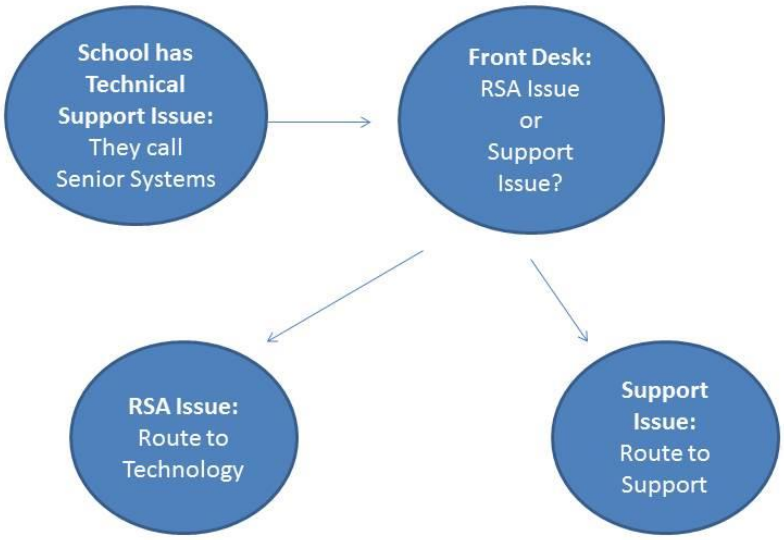
For instance, below I have selected the Accounts Payable application, and entered information for the X3.XA6503 user account with schema PRODUCT:



4. RSA Call Workflow

The RSA Call Workflow process is initiated by a school calling Senior Systems with a Technical Support Issue. The Front Desk determines whether the school's Technical Support Issue is an RSA Issue or a Support Issue. If it is an RSA Issue, the call is routed to Technology. If the call is a Support Issue, the call is routed to Support.

NOTE: To determine if the school's problem is an RSA Issue, the Front Desk simply needs to determine if the school can log into My BackPack with their RSA token. If they cannot log in, then it is an RSA Issue and the call should be routed to Technology. If they can login, then the call is a Support Issue and the call should be routed to Support.



*A standard time period of 48 hours is required for new RSA Token Account requests.

Lost Tokens – If a Faculty member misplaces an RSA Token, call Senior Systems and tell the Front Desk that you have a Lost RSA Token issue. The Front Desk will route you to the Technology Department. Provide Technology with the name of the Faculty Member that lost the RSA token and the serial number of the new RSA Token that you want to assign to this user.

Reassigned Tokens – If an RSA Token must be reassigned to a new Faculty Member, call Senior Systems and tell the Front Desk that you have a Reassign RSA Token issue. The Front Desk will route you to the Technology Department. Provide Technology with the serial number of the RSA Token that you intend to reassign, and the name, Database ID and Cloud User ID of the new Faculty Member.

5. RSA Certification: RSA SecurID Ready Implementation Guide

Last Modified: July 31st, 2013

Partner Information

Product Information	
Partner Name	Senior Systems
Web Site	www.senior-systems.com
Product Name	Advantage Cloud
Version & Platform	My BackPack 925 and higher
Product Description	Everything you need to run your private or independent school. All tied together. Senior Systems provides a comprehensive enterprise-style database system for private and independent K-12 schools. All the pieces work together because all the data is stored in a single, central database. You can get just the modules you need, and you can add more whenever you're ready.

Solution Summary

With Senior Systems, you get the best of both worlds—modular software components give you the flexibility to configure just the system you need, but all the modules utilize a single, central database for seamless integration. You don't have any of the headaches that come with trying to keep multiple copies of data synchronized between applications. Along with improved data integrity, full integration also gives you real productivity benefits, since your staff doesn't need to enter the same data more than once. And full integration means real-time updating, so you know you've got the latest version.

Users of Advantage now have an option for two-factor authentication using RSA Authentication Manager. For this integration, the two-factor's being used are Advantage Cloud password and the tokencode from an RSA SecurID Token. This integration maximizes the protection of data and other resources.

Important: Senior Systems Advantage Cloud is a hosted solution. For technical support, please refer to the Senior Systems Web Site for more information.

RSA Authentication Manager supported features	Senior Systems Advantage Cloud
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes