Aeries Single Sign On (SSO) API Documentation
May 16, 2014

The Aeries API is a web-based, REST API system. Most of the "end-points" for the API are documented in another document: "Aeries API Documentation." This document focuses on the methods for authorized 3rd party vendors to directly point their users to Aeries.net, commonly called a "Single Sign On" solution. This is an incredibly powerful feature and needs to be appropriately secured in your system. The security aspects of this feature can not be understated. You need to critically evaluate the security and safety measures you put in place around this process before you release it to customers. A critical part of this is to not allow a user to input their own Aeries.net Username. If allowed to do so, they could change it to "admin" and then SSO into that account. Not good. Instead, ensure that the Aeries.net Username is something that only a trusted system admin has access to update.

This document is intended for use by vendors wishing to interface with the Aeries API. Interfacing with the Aeries SSO process does not in any way act as an endorsement by Eagle Software (Aeries Software Inc.) of a product. 3rd Party Products are responsible for accurate and secure use of the Aeries SSO process.

Things To Know Before You Begin:

- Read the "Aeries API Documentation" document before you read this document.
- Join the "Interfacing With Aeries" Google Group for updates and information about the Aeries API: https://groups.google.com/forum/#!forum/interfacing-with-aeries

  interfacing-with-aeries+subscribe@googlegroups.com

The Certificate and Security Permissions:

Unless you are an "Eagle Software Elite Partner"(1) and have a certificate issued directly from Eagle Software, each district will issue you a certificate that is unique for that district.

A "certficate" for purposes of interacting with the Aeries API is a 32 character alpha-numeric string.

When a district creates a certificate for a vendor, they can grant access to certain APIs and restrict access to others. This document describes the security area that each end point requires. It would be prudent to document the security areas that you need access to and relay that information to your customers.

It is VERY important to NEVER share or expose your district-issued certificate to end users. That includes being output to the client in Javascript or HTML. All uses of the certificate should be from your server to the district's Aeries.net server.

The Aeries.net demo website can be used to test your code: https://demo.aeries.net/aeries.net/. The certificate for the demo website that you can use is "477abe9e7d27439681d62f4e0de1f5e1". You can also log into the demo website using the username "admin" and password "admin".

Your certificate is case-sensitive!

(1) "Eagle Software Elite Partners" are companies that have formal business relationships with Eagle Software that can involve co-marketing and sales campaigns as well as financial relationships.

Building a Request:

The Aeries API is REST API. Although all current end points use GET requests, POST, PUT, and DELETE actions will be supported in future versions for certain areas.

Request Header:
You will use the Request Header to tell the Aeries API what format you want the response (JSON or XML) and also what your certificate is.

For the response format, include the following:

- XML
  - **Accept: text/xml, text/html, application/xhtml+xml, */***
- JSON
  - **Accept: application/json, text/html, application/xhtml+xml, */***

To give the system your certificate with each request:

- **AERIES-CERT: 477abe9e7d27439681d62f4e0de1f5e1**

The certificate is case sensitive!

How to Interface With the Aeries.net Single-Sign-On Process:

The current Aeries.net SSO process only works for Teachers and Office Staff using the Aeries.net system. It currently does not work for students or parents.

In your system, you will need to create some sort of button or link that triggers the following actions when the user clicks it:

Generate a random character string or GUID. This is the Temporary Authentication Token for this transaction. Next, you will take that Temporary Authentication Token and Pre-Authorize it. Generate an HTTP(s) request to the district's instance of Aeries.net using the following format/example:

https://demo.aeries.net/Aeries.net/api/security/SSO/Init/{UserName}/{TemporaryAuthenticationToken}

Parameters:

UserName - Aeries.net User Name you will SSO in to.

TemporaryAuthenticationToken - the locally generated Temporary Authentication Token. You will need to URL Encode this if the string contains characters like a dash.

Note: Don't forget the "AERIES-CERT" value in the request header!

If successful, the request will return a "String" value looking like this:

XML: <string xmlns="http://schemas.microsoft.com/2003/10/Serialization/">Success</string>

or

JSON: "Success"

If Unsuccessful, the request will return a "401" error.

You may want to log any errors. But from the end user's perspective, you probably want to continue on to the next step no matter what is returned in the Pre-Authorization Step.

Now direct the user to the "LoginDirect.aspx" of Aeries.net. This can be done using a new browser window/tab. A warning to you though... If you try to use JavaScript to open a new window but that JavaScript wasn't specifically run from a user's action (click), then iPads and some browsers may reject the JavaScript command to open a new window.

https://demo.aeries.net/Aeries.net/LoginDirect.aspx?AuthToken={TemporaryAuthenticationToken}&school={SchoolCode}

Parameters:

TemporaryAuthenticationToken - the above mentioned Temporary Authentication Token.

SchoolCode - Optional - can be either the Aeries School Code, State-Defined County-District-School Code (14 digits), State-Define District-School Code (12 digits), or State-Defined School Code (7 digits). If "school" is not passed or the value passed is not valid for the user then the user will be presented a screen to select a school to log in to.

Districts will also need to grant permissions inside Aeries.net to users who can be "SSO-ed". This is done using the Aeries.net Security screens as is the security area called "Single-Sign-On from 3rd Party Systems." Also, the system admin who generates your certificate needs to also give your certificate permission to use the Single Sign On API.

Feel free to test your code against our demo system: http://demo.aeries.net/aeries.net/.