State Data Validation Suite Security Explained

Level Data applications integrate tightly with PowerSchool. These include page enhancement applications like RealTime Validation, and full page applications like State Data Validation and Validation Reporting.

Each of these applications has options available to help District Administrators apply the appropriate security options, as per their district policies and following PowerSchool security guidelines.

This document outline how Level Data's PowerSchool applications integrate with PowerSchool's security mechanisms in order to properly secure the applications.

Plugins

Level Data applications are accessed through the use of three plugins:

- **Level Data Core**: Provides access to Level Data's services and an interface to PowerSchool districts to allow access to Level Data applications.
- **Level Data Core Schema**: Contains the database schemas for the new tables being used by Level Data applications.
- **Level Data Core Schema Permissions**: Maps API level access to Level Data application specific endpoints, to apply access rights to tables installed by Level Data Core Schema plugin.

The preferred method of installing the three plugins is via the **Plugin Management** Dashboard, which can be found under **System Settings**, within the Systems menu in PowerSchool.

Manual installation is still possible, and a previous version of the plugin may have been installed manually on your PowerSchool System (via the custom/web_root directory on the PowerSchool server or Custom Page Management). For information on how to manually remove old plugin versions and installing the latest plugin, please see the "Important Links" section of this document. However, contact Level Data if you require assistance with plugin removal or installation..

Security

Level Data's applications respect PowerSchool's two main security mechanisms: Page Level Security and Field Level Security. Since applications might use one or a mix of both security mechanisms, once installed all Level Data applications should be considered insecure by default.

It is highly recommended that once installed, PowerSchool System Administrator's go through the set up for each of these security mechanisms, to ensure that access to the applications and data, is appropriately set throughout the system.

Level Data's recommended approach is to implement User Access Role based security across the PowerSchool system, while in conjunction, locking down Groups. Allowing the System Administrator to open access to pages or fields as needed, and ensuring that no one is starting out with more access than necessary.

PowerSchool Configuration

To review your current Groups, from the PS start page:

1. Click on **System** within the main navigation menu
2. Under the **Security** click on **Groups**
3. Click on any of the groups available to access its **Edit Group** page.

To review what users belong to specific Groups, from the PS start page:

1. Click on **System** within the main navigation menu
2. Under the **Security** click on **User by Group**

To view and modify the Group/Role a user is assigned to, from the PS start page:

1. Click on the **Staff** tab
2. Select A Staff Member
3. Click on **Security Settings** within the main navigation menu
4. Click on the **Admin Access and Roles** tab
5. Modify the groups that the user is assigned from the **Default Group** dropdown and/or set the roles for the user (per school if desired) through the **Roles and Schools** section

To view and modify Field Level Security, from the PS start page:

1. Click on **System** within the main navigation menu
2. Under the **Security** click on **Field Level Security**
3. Find the fields that need to have their security set and edit them
    - If you cannot find the field that you are looking to set security for, you can click on the **Add** button, which is available at the top-right of the Field Level Security page and add the field if available within PowerSchool's list of managed fields.