Security Roles in Edwin Analytics Table of Contents

Security Roles

Edwin Analytics is accessible to every public school district and charter school through the Department of Elementary and Secondary Education's Security Portal on the Department's website. As with many of the applications on the portal, access is granted locally through the Directory Administration application.

Superintendents, principals, teachers, and other district personnel who want to gain access to Edwin Analytics must contact their district's directory administrator. To find a list of directory administrators in your district or charter school, visit the Department's website for the list of directory administrators.

The following chart provides a quick view of the available roles. However, because of the confidential information available in Edwin Analytics and the laws regulating access to such information, it is strongly recommended that directory administrators read this document completely and consult their superintendent, principal, or charter school leader before assigning these roles.

Security Roles Required:	Edwin Analytics District Administrator	Edwin Analytics School Administrator	Edwin Analytics Evaluator	Global Role: Teacher	Warehouse File Exchange Dropbox
District-wide access to student-level data	X				
District-wide access to teacher evaluation data	X		X		
Student Claiming file upload	X				X
School-wide access to student-level data		X			
School-wide access to teacher evaluation data		X	X		
Classroom-level access for teachers				X	

Security Roles for District and School Administrators

There are two security roles for district and school administrators. These roles are mutually exclusive in that only one role should be assigned to an individual and the role will depend on the user's organization association (district or school) in Directory Administration.

- ***Edwin Analytics District Administrator*** (formerly *DW – (210) District User*) has access to confidential, state loaded student data for their districts. They can also view the analysis cubes using the IBM/Cognos PowerPlay Web application.
- ***Edwin Analytics School Administrator*** (formerly *DW – (211) School User*) has access to confidential, state-loaded student data for their schools. They can also view the analysis cubes using the IBM/Cognos PowerPlay Web application.

These roles also provide access to state loaded *public* data without restrictions, including aggregate data for other schools and districts. *These roles do **not** need to be reassigned if the user was already assigned one of the DW roles.*

The person in the district who will be responsible for student claiming should be assigned the ***Data Warehouse File Exchange Drop Box*** role.

- ***Data Warehouse File Exchange Drop Box:*** This role is assigned to the person who will send the district's "student claim file" (see *Student Claiming* on the Edwin Analytics website). It is available at the district level only and should be assigned in addition to role ***Edwin Analytics District Administrator***.

Adding Evaluator Security Role for District and School Administrators

- ***Edwin Analytics Evaluator*** (formerly *DW – Evaluator*) provides district and school administrators access to classroom reports.

NOTE: You cannot get access to Edwin Analytics with *only* the ***Edwin Analytics Evaluator*** role assigned. This role must be granted in addition to the ***Edwin Analytics District Administrator*** or the ***Edwin Analytics School Administrator*** role but will apply to *all organizations* (districts or schools) associated with any Edwin Analytics roles assigned to the user.

The ***Edwin Analytics Evaluator*** role provides access to the classroom level reports. Edwin Analytics contains several categories of data including student learning, growth, and achievement data that can now be organized by classroom and by teacher. When organized in this way users with ***Edwin Analytics Evaluator*** access can review student achievement data, like MCAS growth data, to draw conclusions about teacher performance. New regulations issued by the Massachusetts Department of Elementary and Secondary Education regulate the manner in which student achievement data can be used to evaluate teacher performance. The regulations indicate that:

"student learning, growth, and achievement data…used…as part of an individual educator's evaluation shall be considered personnel information." 603 CMR 35.11(6).

As such, this data is private, non-public, and superintendents and principals should grant ***Edwin Analytics Evaluator*** access only to educators who have a legitimate business purpose or the responsibility to review "personnel information." This role should only be granted to users who have evaluation responsibility for ***all*** teachers in their authorized organizations.

New Security Role for Teachers

- ***Global Role: Teacher*** was created to allow teachers access to their classroom level information.
- ***Global Role: Teacher*** provides access to student data in the teacher's classrooms as reported in the EPIMS and SCS collections.
- Initially users with this new role will only have access to the new *Teacher* tab and the reports accessible from this tab. They will not have access to the *District*, *School*, or *Students, Staff & Classroom* tabs that ***Edwin Analytics District Administrator*** and ***Edwin Analytics School Administrator*** roles can access.

The steps to assign all security roles are as follows:

1. Add users to the appropriate organizations (school or district) if they have not been added already.

NOTE: ***Data Warehouse File Exchange Drop Box*** and ***Global Role: Teacher*** are available at the district organization level only.

2. Assign *only one* data warehouse security role (***Edwin Analytics District Administrator*** or ***Edwin Analytics School Administrator*** or ***Global Role: Teacher***) to grant a user districtwide, schoolwide, or classroom access. Access issues can arise from having multiple roles assigned.
3. Assign both the ***Data Warehouse File Exchange Drop Box*** role and the ***Edwin Analytics District Administrator*** security role to the user who will be uploading a student claiming file. (See the *Student Claiming* document, for more information on student claiming.)
4. Assign both the ***Edwin Analytics Evaluator*** role and *either* ***Edwin Analytics District Administrator*** or ***Edwin Analytics School Administrator*** security roles—*but not both*—to the user who will be evaluating educator performance. This role should only be granted to users who have evaluation responsibility for ***all*** teachers in their authorized organizations.
5. Ensure that all users read and agree to the district's data access policy as required and explained in the following section on security.

Responsibilities

Confidential Data

According to federal law, a school or district may disclose personally identifiable information from a student's education record without consent to **"**other school officials, including teachers, within the [school or district] whom the [school or district] has determined to have legitimate educational interests**.**" FERPA at 34 CFR § 99.31(a)(1). The standard in Massachusetts is, arguably, even more strict. As described in the state Student Records Regulations at 603 CMR 23.00 (see the definition of "authorized school personnel" in 23.02), no individuals or entities other than the parent, eligible student, or *school personnel working directly with the student* are allowed to have access to information in the student record without the specific, informed, written consent of the parent or eligible student.

Edwin Analytics contains both public and confidential information. Examples of public information include:

- Aggregated school, district, and statewide test results that *do not contain* a list of student characteristics that would make it possible to identify a student's test results
- Staff name, position

Examples of confidential information include:

- Aggregated school, district, and statewide test results that contain a list of student characteristics that would make it possible to identify a student's test results
- Student test results
- Educator evaluation information

When a district, school, or classroom user runs one of the state's predefined reports, only the authorized information for that user's district, school, or classroom is returned, depending on the user's security role and district or school affiliation in Directory Administration, or classroom affiliation in the district certified EPIMS and SCS collections. This conditional access to confidential data also extends to the aggregate data displayed in the state's predefined reports. Report Studio, the IBM/Cognos application used to create predefined reports, supports conditional suppression. However, PowerPlay Web analysis cubes do not support conditional suppression so it is important that users understand the rules regarding the confidentiality of some aggregate data.

Suppressing Aggregate Data for Small Groups

According to federal education laws, confidential information includes "a list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty."[1] Consequently, it is Department policy that public reports containing aggregate student performance data must suppress results for small groups of students when associated with characteristics that would make it possible to identify a student. This policy applies to public reports whenever an identified group contains

- fewer than 10 students for MCAS data or
- fewer than 6 students for SIMS data.

When an identified group is smaller than these thresholds, the report must display a placeholder (for example, -, *, NA) with a disclaimer explaining what the placeholder means. The School/District Profile reports (http://profiles.doe.mass.edu/) provide examples of appropriate suppression.

Predefined reports created by the Department apply conditional suppression rules but PowerPlay Web analysis cubes do not support conditional suppression. Many users who are given access to Edwin Analytics are automatically given access to cubes, therefore, all users should understand small group suppression rules and be careful not to share reports they create from the analysis cubes with unauthorized users.

[1] National Forum on Education Statistics, Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies, NCES. Washington, DC: 2004. http://nces.ed.gov/pubs2004/2004330.pdf

Directory Administrator Responsibility

As explained in the first section of this document, access to Edwin Analytics is gained and controlled by the assignment of security roles in Directory Administration (DA). Within DA, these roles are assigned based on an individual's association with a district or school code. This is not strictly the case in Edwin Analytics. If a user is assigned any of the Edwin Analytics roles (***Edwin Analytics District Administrator***, ***Edwin Analytics School Administrator, Edwin Analytics Evaluator*** or ***Global Role: Teacher***) they will have those roles for ***all organizations*** (schools or districts) that have assigned them any of the Edwin Analytics roles.

Directory administrators should ensure that the user's ID is not being used in another district and should understand that within a district, the 3 roles: ***Edwin Analytics District Administrator***, ***Edwin Analytics School Administrator*** and ***Global Role: Teacher*** need not be assigned in tandem. It is the responsibility of the district's directory administrator(s) to ensure that the security roles for Edwin Analytics are assigned correctly and with proper authority.

Evaluator Role Responsibility

When determining who will receive ***Edwin Analytics Evaluator*** access to Edwin Analytics, superintendents and principals *must* determine which educators on staff have authority to supervise or evaluate *all* teachers who teach in a school. School districts *should not grant* ***Edwin Analytics Evaluator*** access to educators with no supervisory or evaluative responsibilities, or to educators, like department heads or mentor teachers, who evaluate only a subset of the teachers in a school. As necessary, educators with ***Edwin Analytics Evaluator*** access can provide relevant printed or electronic copies of "personnel information" to colleagues who supervise a subset of teachers in the school, and who do not qualify for ***Edwin Analytics Evaluator*** access.

District Data Access Policy

To ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated from Edwin Analytics in violation of state and federal laws and is not used for unauthorized purposes, school districts shall adopt policies governing access and confidentiality of data maintained in Edwin Analytics. Authorized local personnel must participate in training and comply with locally designed confidentiality policies and practices.

Communication and Support

The Department's Edwin Analytics team is working to improve functionality, create new statewide reports, and respond to daily requests from district users across the state. To facilitate communication, the Edwin Analytics team has created the *Edwin Analytics Contact* function (formerly called the *Data Warehouse Contact*) in Directory Administration. The person to whom this function is assigned is the main liaison to the Department. District rollout of Edwin Analytics should be organized so that requests for user support are directed within the district first and only passed to the Edwin Analytics team via the *Edwin Analytics Contact* when it is determined that the issue cannot be resolved locally.

An email list has been created to which all users can subscribe and unsubscribe themselves. This list is two-way so that all users can email the group for support, ideas, and information. Please visit the Edwin Analytics website for information and to subscribe.