



User System and Login Security



Providing access to the Student and Educator portals via any Internet-connected computer provides maximum flexibility, but can also create network security issues. To resolve this, Edgenuity provides options for login and use including **Enhanced Password Security**, **Secure Station**, and **IP Registry** for secure student access.

Edgenuity Enhanced Passwords Security

Edgenuity has signed the Student Privacy Pledge developed by the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA). The provisions require additional security to protect student data against unauthorized third parties access. Edgenuity has added additional security measures of password encryption.

Password encryption converts plain text to unreadable text within Edgenuity preventing the information from being visible within the Student and Educator profile screens. Storing and transmitting encrypted passwords prevents anyone from acquiring passwords and sensitive student data.

Password creation for user accounts can be within any format you wish, and are case sensitive. For security reasons, we recommend against creating passwords with predictable patterns such as student ID numbers. Reset features are incorporated into Edgenuity for Educators assisting users in password retrieval. Additional information regarding passwords is available at [2015-04-10-Password Security and New User Grids](#) and [2015-05-07 – Change Student and Educator Password](#).

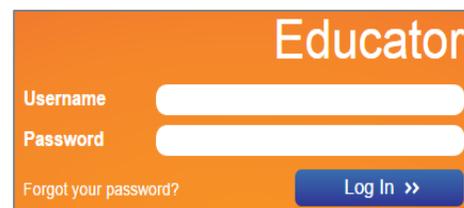
User-Initiated Password Reset

Forgot Your Password

Forgot your password is a self-service feature that can be selected within the Edgenuity login screen should a user be unable to log into their account. Users receive a password reset email to the address on file to regain access.

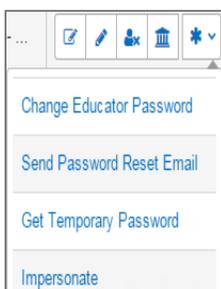
Password reset emails will come from 'noreply@edgenuity.com'. It is recommended to check Junk or Spam folders within your email account if an email is not received shortly.

Please note: Edgenuity does not require a user email address; it is recommended all educators update their Edgenuity account to include a current email address for the password retrieval feature. Alternative options are available should students not have an email address associated with their Edgenuity account.



Educator-Initiated Password Reset Features

Educators with the security permissions can assist student and fellow educator users in regaining access to their Edgenuity account with Change Educator (or Student) Password, Send Password Reset Email, and Get Temporary Password features.



Change Educator (or Student) Password

Change Educator (or Student) Password allows an educator to enter a new student or educator user password.

Send Password Reset Email

A password reset email can be sent if the user account has an associated email address.

Get Temporary Password

Educators can establish a temporary password for users to log in. The user must establish a new password after log in. This feature can be used if you don't want the person changing the password to know the final password.

Please note: When using *Get Temporary Password* the user's original password is removed from the account and will no longer work.

Impersonate

Educators can assist students by logging into the Edgenuity account as the user. Once the account is accessed the educator can view and interact within the system as the user. Impersonation sessions are recorded and logged within Recent Actions similar to other actions that occur within the system.

Please note: When using the Impersonate feature, please be aware of the following:

- A warning will display for an active session if the student is currently logged into their account. Continuing with *Impersonate* will log the student off their active session.
- Contact your Administrator if using the *Impersonate* feature on a computer not previously approved.

* Password encryption does not affect login credentials managed via API, LTI, LDAP, or SAML integration. Users under those integrations sign in with credentials managed by a school and are not maintained by Edgenuity. Passwords will not be overwritten for users with nightly imports where manual password changes may occur.

Edgenuity Secure Station

Providing access to the Student and Educator portals via any Internet-connected computer provides maximum flexibility, but can also create network security issues. To resolve this, Edgenuity provides the option of a proprietary program called Student and Educator Secure Station.

How Secure Station Works

Secure Station provides the ability to secure access, control, and monitor Edgenuity Student and Educator portal environments. Edgenuity School or District Administrator users can allow or deny access to end-users by authenticating specific computer labs or other monitored computer workstations. If access is requested on a workstation not previously authenticated (such as home, a library, media center, or elsewhere), Secure Station can grant or deny entry into the portal.

This process creates a Secure Station White List of verified computers previously authenticated and allowed by the District/School Administrator user. In creating a white list, Secure Station obtains and stores unique identifiers regarding the computer(s) attempting to log in, as well as details about the user. Secure Station then uses the white list containing the unique identifiers to authenticate and grant or deny access to the computer attempting to log into the Student and Educator portals.



Please Note:

Secure Station will not operate within the Chrome™ browser due to Java® reliant features.

To address Java-reliant features within Secure Station for Chrome browser users, Edgenuity offers **Edgenuity IP**

Registry for Secure Student ACCESS. IP Registry provides the ability to secure access, control, and monitor Edgenuity Student and Educator portal environments without use of Java.

Students Logging Into a Secure Station Network

When students log into on a computer where Secure Station has not previously been authenticated, a java applet will appear within the screen to run Secure Station.

Once Secure Station is running, the Edgenuity Security Management System will load the request authentication for the computer being used. Secure Station will then validate the computer workstation, allowing the student to enter into the portal successfully, or denying access to the student based on the authentication process.

Educators Logging Into a Secure Station Network

As an added security option, Edgenuity has also implemented Educator Secure Station. Identical to the Student Secure Station process, the system restricts access to the Edgenuity Educator site to authenticated locations. With Educator Secure Station enabled, students who may inadvertently obtain an educator's login and password will be denied access to the site from unauthorized computers.

Access from Remote Locations Outside of School

In addition to a school's computer lab, students can access their courses from any computer with a high-speed connection via the Edgenuity ASP model. A high-speed Internet connection can provide full access to all associated instructional videos, course materials, and other activities via the web interface for students accessing the portal outside of school. All results and tracking are posted within the Edgenuity School Administration system, allowing teachers to view progress of any student at any time.

Edgenuity IP Registry for Secure Student Access

Google™ Chrome has ended support for Java. Because of this, Edgenuity's Secure Station feature will no longer function for users accessing the Edgenuity portals via Chrome. Users of other browsers such as Internet Explorer®, Firefox®, and Safari® will not be affected and Secure Station will continue to function.

To address this issue for Chrome users, an IP Address Registry feature can be used to ensure students are logging into Edgenuity. This feature allows school administrators to define a registry of IP addresses approved to access the system. Because the new approach will not rely on Java, students accessing Edgenuity from an approved IP address will also be able to access Edgenuity on tablets and Chromebooks.

Secure Station will continue to exist in its current form but will not function on the Chrome browser. Edgenuity's Secure Station for Educators will not be modified at this time, and will continue to function as is in IE, Firefox, and Safari.

What Do I Need To Do?

If you have Secure Station for Students enabled and if your students use the Chrome browser, ***you will need to enable the IP Address Registry feature to replace Secure Station.***

If your students do not use Chrome, or if you don't currently have Secure Station enabled, you do not need to take any action at this time. However, you may choose to implement the IP Address Registry as it has the additional benefit of regulating Edgenuity access from tablets and other devices that don't use Java.

If you have Secure Station for Educators enabled and if your educators use the Chrome browser, ***you will need to identify an alternate browser for Educators to use.***

How Do I Prepare?

Once you've made the following decisions, you are prepared to enable the IP Address Registry.

- ✘ For each school, decide which Educator account holders will be given the user permissions to create and administer the IP Address Registry and individual student bypasses.
- ✘ Educators who currently have the Manage Virtual Classroom Secure Station and Manage Web Admin Secure Station permissions will automatically get the new Manage Student Access Control and Manage Educator Access Control permissions.
- ✘ For each school, determine the IP addresses (or ranges) of the firewall or edge router that represents the 'gateway' to the Internet. You will enter this IP address or range in the Edgenuity configuration page.
- ✘ Decide whether you want students on non-approved IP addresses to be completely blocked from accessing Edgenuity, or to be allowed access to coursework but not assessments.
- ✘ If you have individual students with permission to do coursework and assessments from home, prepare a list of those students. You will be able to put those student accounts on a bypass list that lets them access Edgenuity from outside the block of registered IP addresses.
- ✘ If you currently have Educators using Chrome and want to enforce Secure Station for Educators, decide which alternate browsers you will support for Educators, and inform Educators of this change.

Additional information regarding IP Address Registry is available when logged into the Educator portal. Please contact Customer Support for more information for this feature.

Some software products marketed by Edgenuity and its distributors contain proprietary software components of other software vendors. Internet Explorer is a registered trademark of Microsoft Corporation in the United States and other countries. Safari is a registered trademark of Apple Inc. Firefox is a registered trademark of the Mozilla Foundation. Google, and Chrome are trademarks or registered trademarks of Google Inc. Java is a registered trademark of Oracle and/or its affiliates.

