

Users and Permissions

Slate supports unlimited user licenses, so anyone at your institution who needs Slate access can be added as a user. Security Administrators are able to add and maintain users and grant access to specific Slate resources through the User Permissions module.

How to Add Slate Users

1. Navigate to the Database module. (Click the  icon.)
2. Click [User Permissions](#).
3. Click **New User**

New User

User	Roles	Permissions	Details
First Name	Marrienne		
Last Name	Smith		
Preferred/Short Name	Mary		
Email	msmith@technolutions.com		
Primary Phone	203-404-4835		
Mobile Phone			
Title	Admissions Officer		

Security

User Type	User
User ID	msmith
Home Country	United States
Active	☒ Enable account for access.
Supervised	☐ Require supervised login from non-supervised account.
Expires After	

Select User. See explanation below.

Important: The User ID must match the single sign-on ID (e.g., NetID, authentication ID) users regularly use at your institution.

If you have users based outside of your institution's country, select the country where the user will access Slate most often.

Check the Enable account box.

 **Un-Enable Accounts**
Simply uncheck the Enable box if a user no longer needs access to Slate.

The Supervised checkbox is typically used for student workers. See the end of this section for more information.

You may optionally enter a date after which this account will automatically deactivate.



What are the User Type options?

User

People who have institutional accounts (e.g., NetIDs) and need to access Slate to view or edit student data. This type will be used for the majority of your Slate users.

External User

People who do not have institutional accounts and need to access Slate to view or edit student data (e.g., visiting faculty). Slate authentication will be used for these users.

Service Account

Accounts that need access to Slate SFTP servers only (e.g., vendors).

Users and Permissions (continued)

Roles

Roles can be used to quickly assign a set of permissions to users. When a user is assigned a role, all permissions associated with that role are inherited.



Our Best Advice

Do not add all your possible Slate users at once! Add users and assign permissions as their roles become relevant within Slate.

New User

UserRolesPermissionsDetails

Roles

Role

☒ Administrator (All Access)

Exclusive Permissions

Permission	Status	Code
☐ Direct SQL Access		sql_direct
☒ Security Administrator		security
☐ SFTP Access		sftp
☐ SSN Unmask		ssn
☒ Submit requests to Service Desk		ticket

Typically, an institution will assign the Administrator Role to the members of their core Slate team (e.g., the Slate captains).

Exclusive permissions cannot be inherited from Roles and must be granted on this tab. (See upcoming page for more information about Exclusive Permissions.)

Grant the Security Administrator permission to users who will maintain Slate users for your institution.

Grant your Slate Captains the permission to Submit requests to Service Desk.

Administrator is a standard role that is assigned all permissions on the Permissions tab. When a user is assigned this role, the user will inherit all non-exclusive permissions, including custom permissions.

New User

UserRolesPermissionsDetails

Permissions [More Information](#)

Permission	Status	Code
☒ Application Decide	Granted	appdecide
☐ Application Lookup	Inherited	applookup
☐ Application Lookup (Active Period Only)	Inherited	applookup_active
☒ Application Update	Granted	appupdate
☐ Audit Log		audit
☐ Batch Acquire		acquire
☐ Bin Management	Inherited	bin_management

Permission statuses include:

Inherited

The permission has been granted based on a Role.

Granted

The permission is explicitly selected on the Permissions tab.

Blank

The user does not have this permission.

Users and Permissions (continued)



Slate Exclusive Permissions

Exclusive Permissions can never be inherited. These permissions must be set on the Roles tab for a Slate user.

Direct SQL Access

Slate supports direct, native SQL Server connections that may be used from any client that supports connections to a SQL Server. The connections provide a read-only interface into your Slate database.

Direct SQL Access

[Connection Instructions](#)

Review more in-depth instructions in the Slate Information Network.

Host sql.technolutions.net

Cluster flora

Database slate-demo

Username slate_slate-demo_user

Password Not Set [Reset Password](#)

Click Reset Password to set the password for the first time, and record this password for future use. You **will not** be able to see this password again once you close the popup window.

Allowed Networks

Allow 60 minutes for any changes to take effect.

1.2.3.4, 123.123.123.0/24

Enter individual IP addresses or CIDR subnets (e.g., 140.247.0.0/16) separated by commas. The IP address of your current machine is 1.2.3.4.

Enter the IP addresses the user will use to connect to the SQL server. It can take up to an hour for the whitelist to take effect.

Security Administrator

A school must have **at least one** designated Security Administrator.

Manage Slate Users: A Slate user must have this permission in order to add and edit Slate users.

Monitor Slate Usage: If a user attempts to login from an unrecognized location that is outside of the school's home country and in a country that has not been visited by this user within the past 30 days, an email notification will be generated to the email address on record for the user, requiring the user to verify the login by clicking on a link. A separate notification will be sent to **all security administrators** for the instance.

If the user **allows** the login, he or she may proceed as normal, and there will be no additional verifications for that user when he or she logs in from that country, so long as that user's access in that country does not idle for more than 30 days.

If the user **denies** the login as unauthorized, an additional, high priority email will be sent to the user and to **all security administrators** for the database reporting the unauthorized login attempt.

These checkpoints are part of a comprehensive security strategy to identify suspicious activity and behavior.

Users and Permissions (continued)



Slate Exclusive Permissions (continued)

SFTP Access

SFTP is an extension of the Secure Shell protocol (SSH) to provide secure file transfer capability. SFTP supports authentication through either a username/password pair or a username/certificate pair. With certificate-based authentication, which is considerably more secure than password-based authentication, your institution will need to generate an SSH certificate pair that will be used when authenticating.

SFTP Access	Connection Instructions
Protocol	SFTP
Host	ft.technolutions.net
Port	22
Username	demo@demo.technolutions.net
Command Line	sftp demo=demo.technolutions.net@ft.technolutions.net
Password	Not Set Reset Password Clear Password
SSH2 Public Key	--- BEGIN SSH@ PUBLIC KEY --- Comment: "" AAAAB3NzaC1yc2EAAAABJw/RSHfOxbin...
Path Restriction	/incoming/frontrush /outgoing/frontrush Enter absolute paths, like /incoming/ or /outgoing/, separated by lines to restrict a user's access to specific folders.
Allowed Networks	1.2.3.4, 123.123.123.0/24 Allow 60 minutes for any changes to take effect. Enter individual IP addresses or CIDR subnets (e.g., 140.247.0.0/16) separated by commas. The IP address of your current machine is 1.2.3.4.

Review more in-depth instructions in the Slate Information Network.

Optional: Click Reset Password to set the password for the first time, and record this password for future use. You **will not** be able to see this password again once you close the popup window.

This should be an SSH2 public key, which will typically begin with

"--- BEGIN SSH2 PUBLIC KEY ---"

and end with

"--- END SSH2 PUBLIC KEY ---".

Optional: Restrict the paths that a user may access. This setting can be especially useful for vendor service accounts.

Enter the IP addresses where SFTP connection requests will originate. It can take up to an hour for the whitelist to take effect.

SSN Unmask

Social Security Numbers are masked by default in Slate. This permission grants access to unmask the SSN.

Social Security Number [Unmask](#)

Users with the SSN Unmask Exclusive Permission will see this link to view the full Social Security Number.

Submit Request to Service Desk

Up to three users may have the permission to submit service desk requests to Technolutions. This exclusive permission should be reserved for Slate Captains only. This is to ensure that requests are submitted and ranked according to the institution's priorities, rather than many separate individuals' priorities.

Users and Permissions (continued)



Slate User Permissions

Application Decide	Add, Confirm, Assign Letters, and Release decisions individually from the application record. Also grants access to Decision Management if the user has read access for a query.
Application Lookup	Grants read access to view all data on an application tab within the student record.
Application Lookup (Active Period Only)	Grants read access to view all data on an application tab within the student record if the application is associated with an active application period.
Application Update	Grants write access to application data, including updating the application round, application-scoped fields, submission status, activities, and checklist items.
Audit Log	Grants access to view the Audit Log for a student record.
Batch Acquire	Grants access to upload documents and associate them with a record within Batch Acquire.
Bin Management	Grants access to the Bin Management tool to batch assign reader bins and queues for applications included in a query. The user must also have read access to the query.
Consolidate Records	Grants full access to the Consolidate Records tool, including the compare tool and the ability to merge records that appear as potential matches.
Custom SQL	Grants the ability to view and edit the SQL tab within the Form Builder; create and edit custom SQL queries; create and edit individual custom SQL exports and filters in the Query Builder tool.
Database	Grants access to all Admin Tool items; Ping; Decision Letters; Application Editor; Standard Query Library
Deliver	Create Deliver messages and edit Deliver messages associated with the user account; Grants access to the Email Gateway Inbox to view emails sent by this user.
Deliver (edit all users)	Create Deliver messages and edit any Deliver message, regardless of the user; Grants access to the SMS Inbox and the Email Gateway Inbox to view messages sent by any user.
Deliver Send	Send or stop Deliver messages.
Event Registration	Create events, access and edit events associated with the user account.
Event Registration (edit all users)	Create events, access and edit any event, regardless of the user.

Users and Permissions (continued)



Slate User Permissions (continued)

Financial Aid	Grants access to the Financial Aid checklist and the Financial Aid query folder.
Form Builder	Create forms, access and edit forms associated with the user account.
Form Builder (edit all users)	Create forms, access and edit any form, regardless of the user.
Import	Grants access to import files using Upload Dataset.
Inbox	Grants access to Message Inbox.
Interactions	Grants access to the Timeline tab on the student record.
Person Lookup	Grants read access to view a student record.
Person Lookup (Active Only)	Grants read access to view a student record that is configured as Active (see the Rules Recipe Book).
Person Update	Grants write access to person data, including updating biographical data, interactions, and person-scoped fields.
Predict	Grants access to Predict.
Query	Create queries and run or edit queries associated with the user account.
Query (edit all users)	Create queries and run or edit any query, regardless of the user.
Query (Slate Template Library)	Grants access to Export and Filter resources in the Slate Template Library while using the Query Builder.
Reader	Grants access to the Reader.
Reader Classify	Grants access to Classify within the Reader.
Refund Maestro Payments	Refund payments made using Maestro within 60 days of the transaction.
Release Decisions	Grants access to the Release Decisions module - including the ability to confirm decisions, assign letters, and release decisions in batch.
Rules Editor	Grants access to the Rules Editor.
Scheduler	Create interview slots, access and edit interviews associated with the user account.
Scheduler (edit all users)	Create interview slots, access and edit any interview, regardless of the user.
Service Desk Forums	View the Technolutions Forums, including the Feature Requests Forum, Slate Scholar, and Slate TV.
Service Desk Requests	View service desk requests associated with your institution.

Users and Permissions (continued)



Use Roles to Manage Permissions for a Group of Users

If a group of Slate users have the same work tasks, use a Role Group with necessary Role Permissions as a shortcut to give multiple users the same set of permissions.

How to make a Role Group

1. Navigate to the Database module. (Click the  icon.)
2. Click [Role Groups](#) and then [Insert](#).

Insert Record in Role Groups

Name

Give your Role Group an intuitive name that describes the population of users who use Slate for the same tasks.

In this example, this Role Group will be used for Slate users who are athletic coaches.

Then associate the permissions that belong to the group.

How to make Role Permissions

1. Navigate to the Database module. (Click the  icon.)
2. Click [Role Permissions](#) and then [Insert](#).

Insert Record in Role Permissions

Role

Permission

Select a Role Group.

Select a permission that should be associated with this Role Group.

Add other permissions for a Role Group by inserting additional Role Permissions:

Role	Permission
Insert	
Coach	Application Lookup (Active Period Only)
Coach	Event Registration
Coach	Person Lookup (Active Only)

Custom Role Groups appear on the Roles tab. Select the role for users that should inherit that role's permissions:

New User

User

Roles

Permissions

Details

Roles

Role

- ☐ Administrator (All Access)
- ☒ Coach



Easy Role Management

A user may be assigned multiple Roles (e.g., Coach and Faculty). Additionally, a user may be assigned permissions outside of Role Groups.

If you need to make future permission adjustments for a Role Group, the inherited permissions for all users in that Role Group will be updated automatically.

All permissions associated with this role will be inherited by the user.

Users and Permissions (continued)

Custom Permissions

In addition to the Slate standard permissions, you may create any number of custom permissions. Use a custom permission to grant access to a specific data point (e.g., a field) or business process (e.g., a query) in Slate.

1. Navigate to the Database module. (Click the  icon.)
2. Click [Custom Permissions](#).
3. Click [Insert](#).

Insert Record in Custom Permissions

ID	
Status	Active ▼
Name	Processing



Our Best Advice

Review the Slate standard permissions – and the high-level functions that those permissions grant access to – before you begin making custom permissions.

Custom permissions are most useful when there is a need to have fine-tuned access controls for certain items.

Slate will assign an ID after you save your custom permission.

Set the status to Active.

Give your custom permission an intuitive name.

Custom Permissions appear at the bottom of the Permissions tab when configuring a Slate user:

☐ Scheduler (edit all users)	interview_all
☐ Service Desk Forums	forums
☒ Service Desk Requests	requests
☒ Processing	Granted

Update **Cancel**

Click the box to grant a user a custom permission.

Users and Permissions (continued)

How to Use Custom Permissions

A custom permission may be set when configuring a precise data element within Slate like a field or a Reader Bin. Additionally, a custom permission may be added when configuring the Sharing Permissions for items including queries, forms, and events.

When working on a query or a form, click **Sharing Permissions** to customize the access settings for that function:

Share Permissions

Grantee	Permissions	Status
Add Grantee		

Click Add Grantee to customize access setting for a certain function.

Configure sharing settings for that function:

Edit Grantee

Active

Active ▼

Type

Permission ▼

Permission

Processing ▼

Select Active.

Select the Type. In this example, access is being set for users with a specific permission. (See below for more information.)

Select the specific permission. In this example, access is being granted to users with the Processing custom permission.

Additional configurations will appear based on the Slate module you are using.



What are my Permission Type Options?

User

Grant access for a specific Slate user.

Dataset

Grant access for all records within the selected Dataset.

Dataset Row

Grant access for a specific record within a Dataset.

Permission

Grant access to any user with a selected standard or custom permission.

Role

Grant access to any user assigned to a selected Role.

Users and Permissions (continued)

User Details

You may optionally add notes and export codes on the Details tab.

New User

User	Roles	Permissions	Details
Notes This is a service account for our external vendor.			
Export Value Export Value 2 Export Value 3 Export Value 4 Export Value 5			

Add helpful notes about the user.

If you need to export user data to external systems, you may configure up to five export values.

Supervised Login

The Supervised user setting can be useful if you have student workers who should only be able to access Slate from a computer in your office.

Supervised ☒ Require supervised login from non-supervised account.

This setting is on the User tab when configuring a Slate user.

Logging into Slate as a supervised user is a two-step process:

- 1 A non-supervised staff member must click the **Supervised Login** link on the Slate homepage.



Welcome, Mary Smith.

[Details](#) [Supervised Login](#)

Click the Supervised Login link.

- 2 Copy the URL from the popup window to the clipboard. Close all browser windows. Open a new browser window and paste in the saved URL. The supervised user (e.g., a student worker) may then use their own credentials to log into Slate.