NEW YORK STATE | Office of Mental Health

Authentication User Guide for Internal User

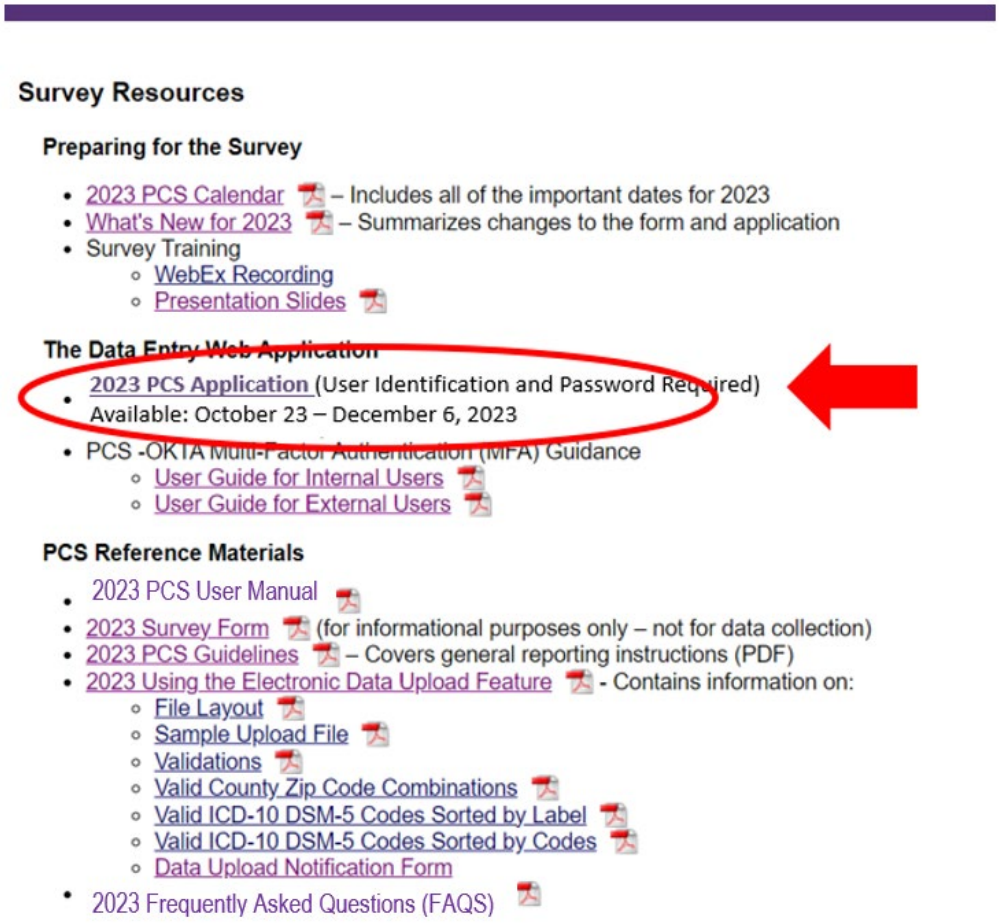
1. Purpose

The purpose of this user guide is to document the steps that are required for the internal users to authenticate to the OMH Applications.

2. Login Process Using a Passcode for Internal Users (State Employees)

The applications that are classified as a passcode-based application will only allow the user to login with the user ID and passcode.

2.1 The user goes to the PCS homepage https://omh.ny.gov/omhweb/pcs/submissions/ clicks on the PCS application link



Survey Resources

Preparing for the Survey

- 2023 PCS Calendar – Includes all of the important dates for 2023
- What's New for 2023 – Summarizes changes to the form and application
- Survey Training
  - WebEx Recording
  - Presentation Slides

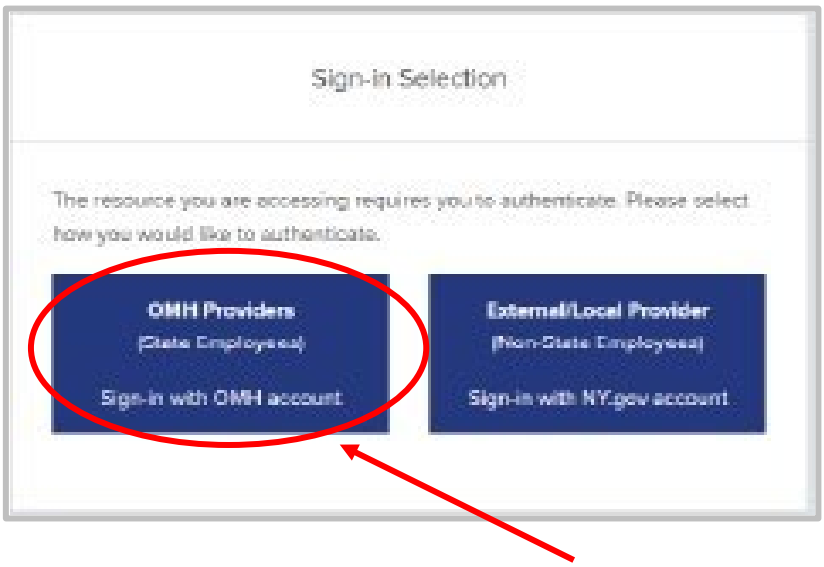
The Data Entry Web Application

- 2023 PCS Application (User Identification and Password Required)
  Available: October 23 – December 6, 2023
- PCS -OKTA Multi-Factor Authentication (MFA) Guidance
  - User Guide for Internal Users
  - User Guide for External Users

PCS Reference Materials

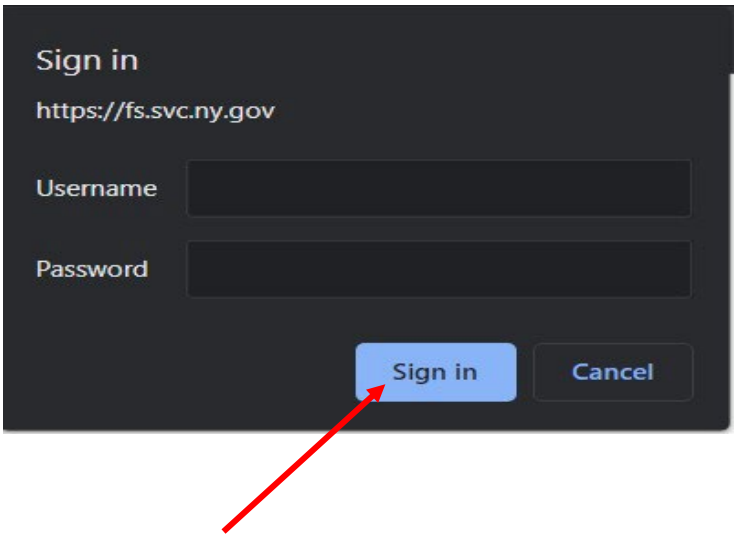
- 2023 PCS User Manual
- 2023 Survey Form (for informational purposes only – not for data collection)
- 2023 PCS Guidelines – Covers general reporting instructions (PDF)
- 2023 Using the Electronic Data Upload Feature - Contains information on:
  - File Layout
  - Sample Upload File
  - Validations
  - Valid County Zip Code Combinations
  - Valid ICD-10 DSM-5 Codes Sorted by Label
  - Valid ICD-10 DSM-5 Codes Sorted by Codes
  - Data Upload Notification Form
- 2023 Frequently Asked Questions (FAQS)

2.2 The user is navigated to the “Sign-in Selection” landing page.



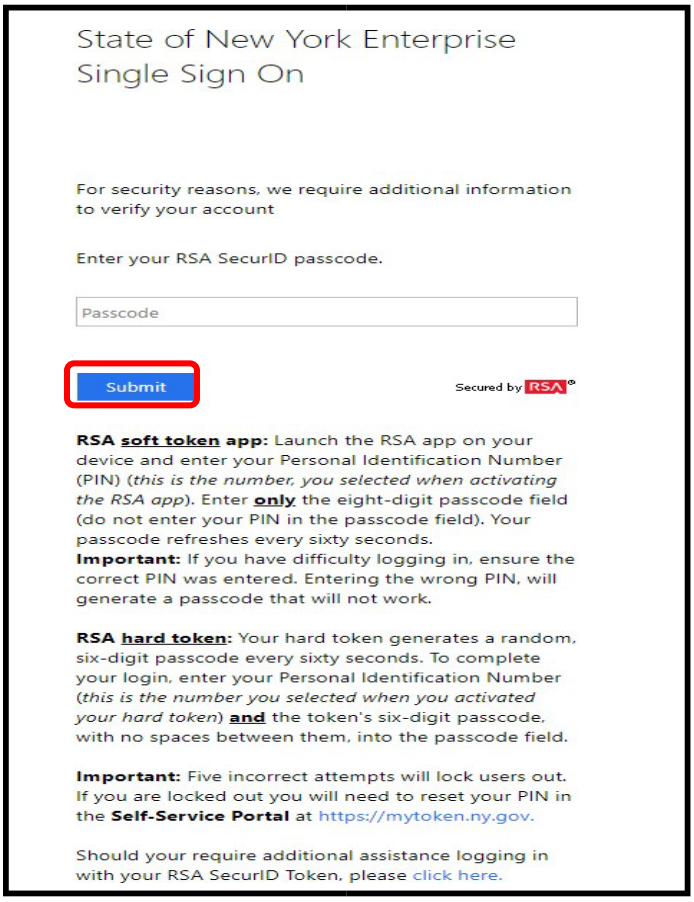
2.3 The user selects sign-in with “OMH Providers (State Employees) Sign-in with OMH account” button to authenticate.

2.4 The user may be prompted to enter his/her username and password.



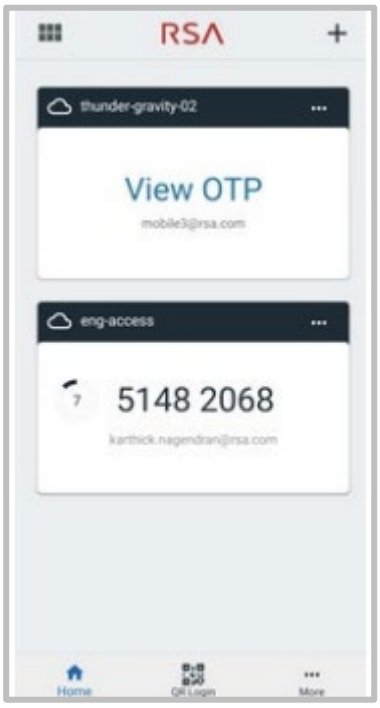
2.5 The user clicks on “Sign in” button.

2.6 The user is then prompted to enter the passcode either from their hardware or software token. The passcode will be masked.



2.6.1 The user logging in using a hardware token enters the 8-digits personal PIN followed by the 6-digit number from the SecureID hard token in the passcode field and clicks on the “Submit” button or presses enter on the keyboard to continue.

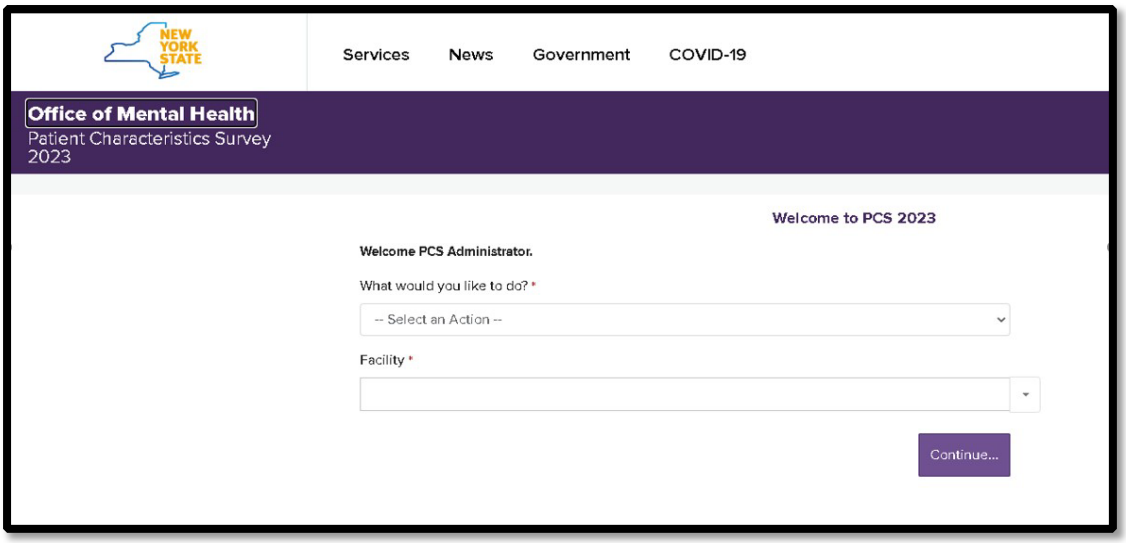
2.6.2 The user logging in using a software token enters the 8-digit personal PIN in the SecureID authenticator app then clicks on submit to get the passcode generated. The user enters the 8-digit code from the SecureID authenticator app in the passcode field and clicks on “Submit” button or presses enter on the keyboard to continue.



NOTE 1: The 6 to 8-digit number generated in the SecureID RSA hardware or software Token will change every minute. A timer on the left side of the token counts down the seconds until the next number will appear. Before the token code changes, be sure to enter the displayed code and submit. Otherwise, it will be out of synchronization with the server and an error message will occur.

NOTE 2: Make sure the personal pin entered is valid for the token being used.

2.7 Upon successful authentication, the user is directed to the PCS application homepage.



3. Glossary

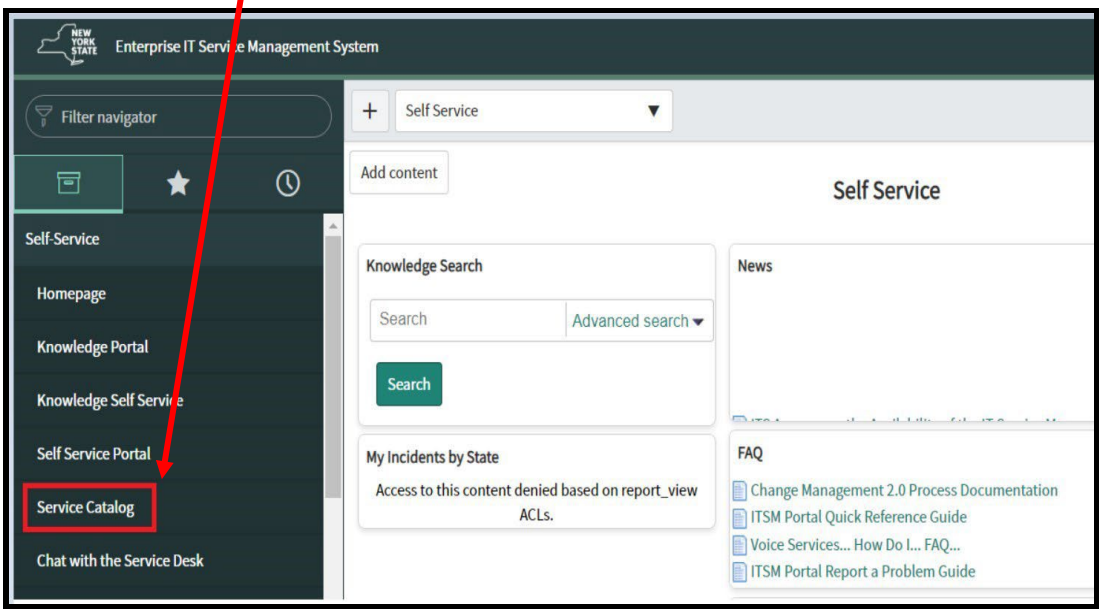
Term	Description
AAL	Authenticator Assurance level.
PIN	Personal Identification Number. 8-digit number that represents “something you know” factor.
	Note-This must be at least 8-digits number to achieve AAL2.
Token Code	Token code is a number generated by the RSA SecurID token every minute. This code represents the “something you have” factor. 6-digit code generated by the hardware device. 8-digit code generated by the RSA SecurID software token.
Passcode	Passcode is PIN plus the token code.
UPN	User Principal Name
Username	User’s User Principal Name (UPN) assigned in Active Directory. User’s short name (sAMAccountName) will also work. UPN is the preferred identifier.

4. Process to create an ITSM incident Ticket

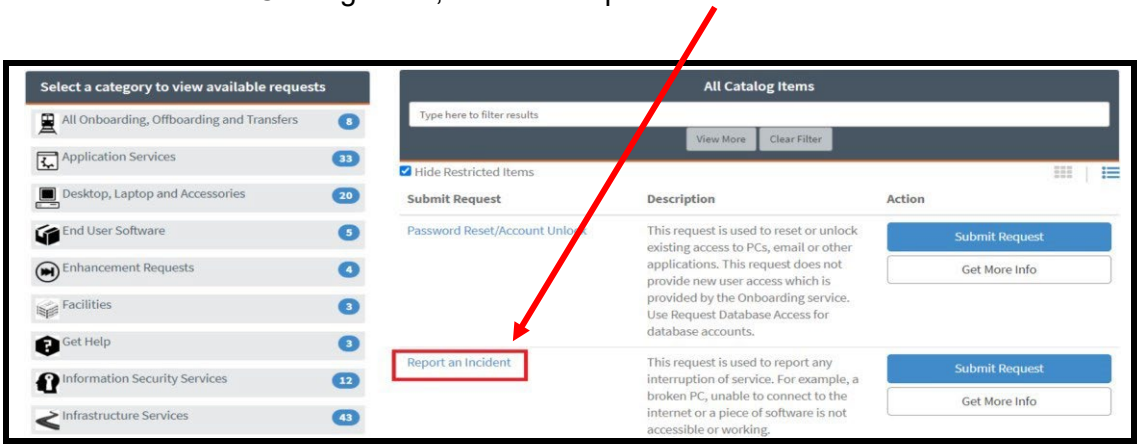
The incident request is used to report any interruption of service. For example, the user not able to log in, password issues, token issues, unable to connect to the internet or a piece of software is not accessible or working.

4.1 Navigate to ITSM to create an ITSM incident ticket.

4.2 Click on Service Catalog from the left-hand menu.



4.3 From the Service Catalog items, click on “Report an Incident”



4.4 The incident request form opens. Use the following guidelines to complete the incident form:

Item	Value
Location	NYS Office of Mental Health
Short Description	Name of the Application (I.e., BHAAS) and Brief summary of the request.
Reported Issue	Select one from the drop-down list below: Application/Software issue Email issue Desktop/Hardware Issue Print issue Telephony Issue Mobile Issue Unknown Issue
Full Description	Full description of an incident; and also include this ticket should be assigned to L3 ISO TSOPSEC OMH.
Impacts	Single User or Multiple Users
Attachments	Add any desired attachments to support the description of an incident.

4.5 Once the entire form has been completed, click submit. Once completed, a summary screen will appear with the **INC#.** You should also receive an email with complete details.