# Obtaining Access to the Message Validation, Processing, and Provisioning System (MVPS) Portal
# Guide for New Jurisdiction Users

Last update: June 24, 2025

## Table of Contents

## Purpose

This job aid provides guidance for jurisdiction personnel on how to obtain access to the MVPS portal.

## Learning Objective

This job aid will provide jurisdiction personnel with guidance on how to request and obtain access to MVPS, review the various jurisdiction user roles available within the MVPS portal, and identify which jurisdiction staff need to be assigned the specified roles and access to the MVPS portal.

## Background

MVPS receives case data from jurisdictions, validates and processes data, and provisions data to CDC programs for their national surveillance efforts.

Jurisdiction surveillance and informatics staff will need MVPS access to:

- monitor case notification submissions from HL7 and legacy methods,
- assess and improve the quality of the data by managing warnings and errors,
- verify low-incidence cases,
- address retired event codes,
- perform case deletions when no other method is available to the jurisdiction, and
- perform annual data reconciliation processes, including final approval of data by the State or Territorial Epidemiologist.

MVPS receives NNDSS data in four message types:

- HL7 – newer HL7 format defined in the Generic version 2 Message Mapping Guide (MMG) and disease-specific MMGs based on Generic version 2
- Legacy formats:
    - Legacy HL7 – older HL7 formats including Generic version 1, Arboviral, and older versions of Tuberculosis (TB) and Varicella
    - NBS – National Electronic Disease Surveillance System (NEDSS) Base System Master Messages
    - NETSS – National Electronic Telecommunications System for Surveillance files.

Jurisdictions are transitioning from sending case notification data in the legacy message types to transmitting in Generic-v2-based HL7. The process of receiving approval to send the HL7 case notification messages is called **onboarding**.

Members of a jurisdiction onboarding team require MVPS access to verify their case notification submissions in MVPS. Jurisdiction staff who will need MVPS access during onboarding may include the:

- project lead,
- lead for integrated surveillance system,
- person responsible for gap analysis,
- person responsible for creating electronic messages,
- person responsible for configuring message transport, and
- person responsible for data administration of surveillance system for conditions covered by a selected MMG.

## MVPS Jurisdiction Roles

The MVPS Jurisdiction Data Manager (JDM) role manages jurisdiction user access to the MVPS portal. It is important that the JDM provides jurisdiction users with the appropriate MVPS access based on their role within the jurisdiction. CDC requires jurisdictions to designate at least two JDMs.

The four MVPS user roles available to jurisdiction portal users are shown in Table 1.

**Table 1—MVPS Jurisdiction Roles**

| Jurisdiction Data Manager (JDM) | Jurisdiction User | State/Territorial Epidemiologist | Sexually Transmitted Diseases (STD) Manager |
|---|---|---|---|
| • Views date for one or more conditions | • Views data for one or more conditions | • Views data for all conditions | • Views data for STD conditions |
| • Receives access to optional MVPS features as assigned by a JDM | • Receives access to optional MVPS features as assigned by a JDM | • Has access to the MVPS reconciliation module<br>• Receives access to optional MVPS features as assigned by a JDM | • Has access to the MVPS reconciliation module<br>• Receives access to optional MVPS features as assigned by a JDM |
| • Works with CDC to set up new MVPS users<br>• Edits user permissions to view conditions and access optional MVPS features | • N/A | • Represents lead state or territorial epidemiologist<br>• Signs off on final tables for all conditions during annual data reconciliation | • Signs off on final STD tables during annual data reconciliation |

A JDM may perform the following functions to assist jurisdiction users in obtaining the proper role-based access in MVPS:

- Identify new users and email their role/contact information to the CDC Electronic Data Exchange (EDX) mailbox at edx@cdc.gov with the subject line "MVPS new user" to request that CDC grants them MVPS access.
- Verify or assign user permissions to conditions (event codes).
- Verify or assign access to features within the MVPS portal, such as low-incidence case verification and delete a case.
- Deactivate jurisdiction users when MVPS access is no longer needed.

The JDM may assign jurisdiction users additional permissions and settings such as: delete a case, low incidence including notifications and reconciliation.
MVPS has two environments available to jurisdiction users, the **onboarding** environment and the **production** environment. The MVPS onboarding environment is only used while jurisdictions are involved in an onboarding process. Once the jurisdiction has finished onboarding, case notification data are transmitted and managed through the MVPS production environment. Most jurisdiction user roles can be assigned in both the MVPS onboarding environment and the production environment. The State or Territorial Epidemiologist role only applies to the production environment.

## Requesting Access to MVPS

If a jurisdiction user requires access to the MVPS portal, a JDM should make the request by sending an email with the subject line "MVPS new user" to the EDX mailbox (edx@cdc.gov). The email should include the new user's name(s), email address(es), and desired MVPS role(s). The conditions (event codes) a user has access to will be assigned later, once the user has portal access, by a JDM.

Alternatively, a jurisdiction user may request MVPS access by sending an email to the EDX mailbox. To streamline the process, the jurisdiction user should include an approval email from a JDM along with the initial request. If an approval email is not provided, CDC will request confirmation from a JDM. If a new user does not know who their JDMs are, they should send an email with the subject line "MVPS access" to the EDX mailbox at edx@cdc.gov.

New jurisdiction users must go through two CDC security steps to access and use the MVPS portal:

**Step 1: Secure Access Management Services (SAMS) Authentication**

- SAMS is used to authenticate users for access to CDC systems, including MVPS.
- SAMS Level 2 authentication (or higher) is required to access the MVPS portal.

**Step 2: MVPS Authorization**

- MVPS ensures that users only have access to the data and activities within MVPS for which they are approved.
- Once a user is authorized to access MVPS, the user will see link(s) for the MVPS production and/or onboarding environments listed under "My Applications" in SAMS.

## Obtaining SAMS Access to MVPS

All jurisdiction users must have a SAMS Level 2 account (or higher) to access MVPS. Those users with a SAMS Level 1 account, the level required for National Electronic Telecommunications System for Surveillance (NETSS) file upload, must request SAMS Level 2 authorization.

After the jurisdiction user sends a request for MVPS access to the EDX mailbox, CDC will initiate one of the following processes:

- If a jurisdiction user is new to SAMS, the user will receive an invitation email from SAMS requesting *primary* and *secondary* forms of ID to complete the identity proofing process.
- If a jurisdiction user has a SAMS Level 1 account, the user will receive an email from SAMS requesting a *secondary* form of ID to complete the Level 2 identity proofing process.
- If a jurisdiction user already has a SAMS Level 2 (or higher) account, the user will be added to MVPS with no additional identity proofing needed.

Users with no prior SAMS account or a SAMS Level 1 account must complete the following steps:

- The user will receive an email from SAMS-no-reply@cdc.gov with the subject "U.S. Centers for Disease Control (CDC): SAMS Partner Portal – Identity Verification Request."
- The email will have guidelines for the identity proofing process to facilitate an initial request or upgrade to SAMS Level 2.
- The user must complete the proofing form and upload it along with required supporting ID documents using the link provided. Alternatively, the email provides options for faxing or mailing the proofing form and required supporting ID documents.

SAMS identity proofing guidelines specify the following:

- IDs must be unexpired, and information such as the user's name, address, and contact information must be consistent among all IDs.
- One of the IDs provided must be a photo ID.
- Scanned or photocopied IDs must be legible.

It is important to note that a jurisdiction user's SAMS invitation is customized for the new user and can only be used for a single registration. If a new user is expecting a SAMS invitation and it hasn't arrived, they should check to make sure it did not get flagged by their email anti-spam filter.

A new jurisdiction user must register with SAMS **within 30 days** of receipt of the SAMS invitation or it will expire. If an issue arises with the SAMS identity proofing process, SAMS may grant a 30-day extension to complete the process. If a new user loses their SAMS invitation or if it expires, they should contact their JDM to request a replacement. A new user can also contact the SAMS Help Desk at samshelp@cdc.gov.

The invitation email from SAMS offers an additional choice to use a third-party Experian identity verification process to register with SAMS. The Experian process is completed online and does not require the user to submit identity proofing documents. By entering profile information and answering a series of questions, a user's identity may be verified in a matter of seconds. This enables the user to quickly proceed to SAMS account activation and/or MVPS access. For additional information on the Experian process, please see the Identity Verification Overview document located at the bottom of the page sams.cdc.gov home page.

When a new user is registered in SAMS and authorized for MVPS access, the user will receive an email from the SAMS help desk indicating the user is approved in SAMS for the MVPS activity and providing the MVPS link(s). When the user logs in to SAMS, the MVPS links should be listed in "My Applications."

Additionally, when a new user is added to MVPS, a designated JDM should assign the appropriate MVPS permissions, settings, and notifications for the new user.

Any additional questions about registering with SAMS or accessing MVPS links via SAMS should be directed to:

SAMS Help Desk
Monday-Friday, 8:00AM to 6:00PM EST
Excluding U.S. Federal Holidays
877-681-2901
samshelp@cdc.gov

Jurisdiction users or JDMs may also email questions to the EDX mailbox at edx@cdc.gov with the following subject lines:

- For an MVPS New User request: "MVPS new user"
- For a general MVPS access inquiry: "MVPS access"
- For a general SAMS related inquiry: "SAMS access

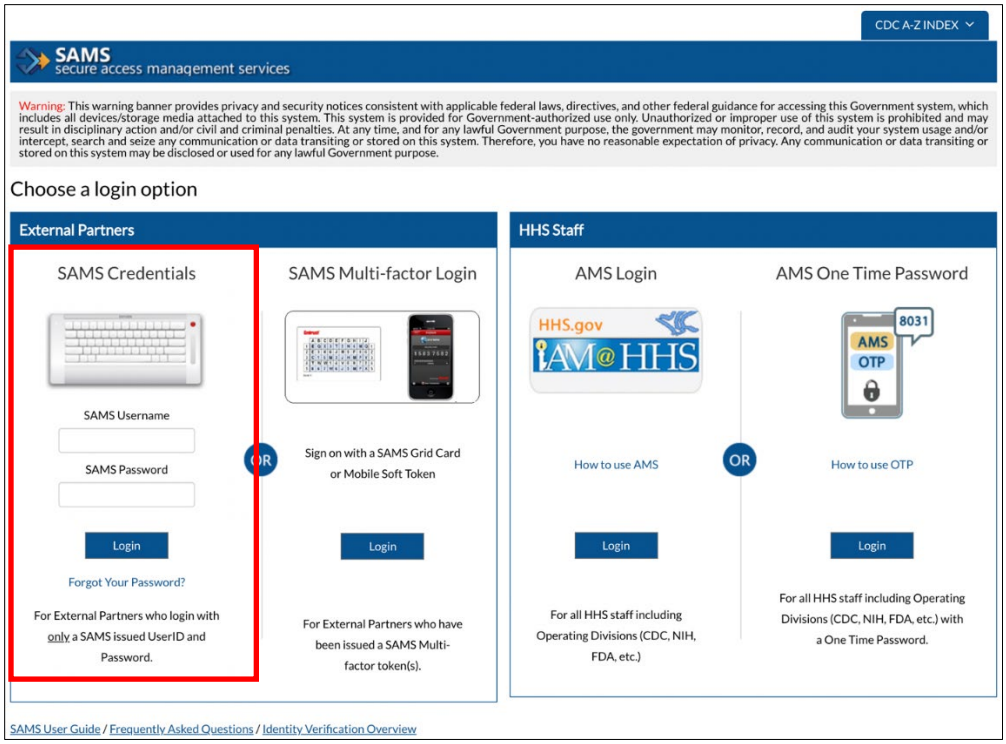
## Logging in to the MVPS Portal

To log in to the MVPS portal, users should follow the two steps shown below.

**Step 1**: Access MVPS via SAMS (Figure 1) using either of the links below and enter your SAMS credentials (SAMS username and SAMS password):

https://sams.cdc.gov
https://mvps.cdc.gov

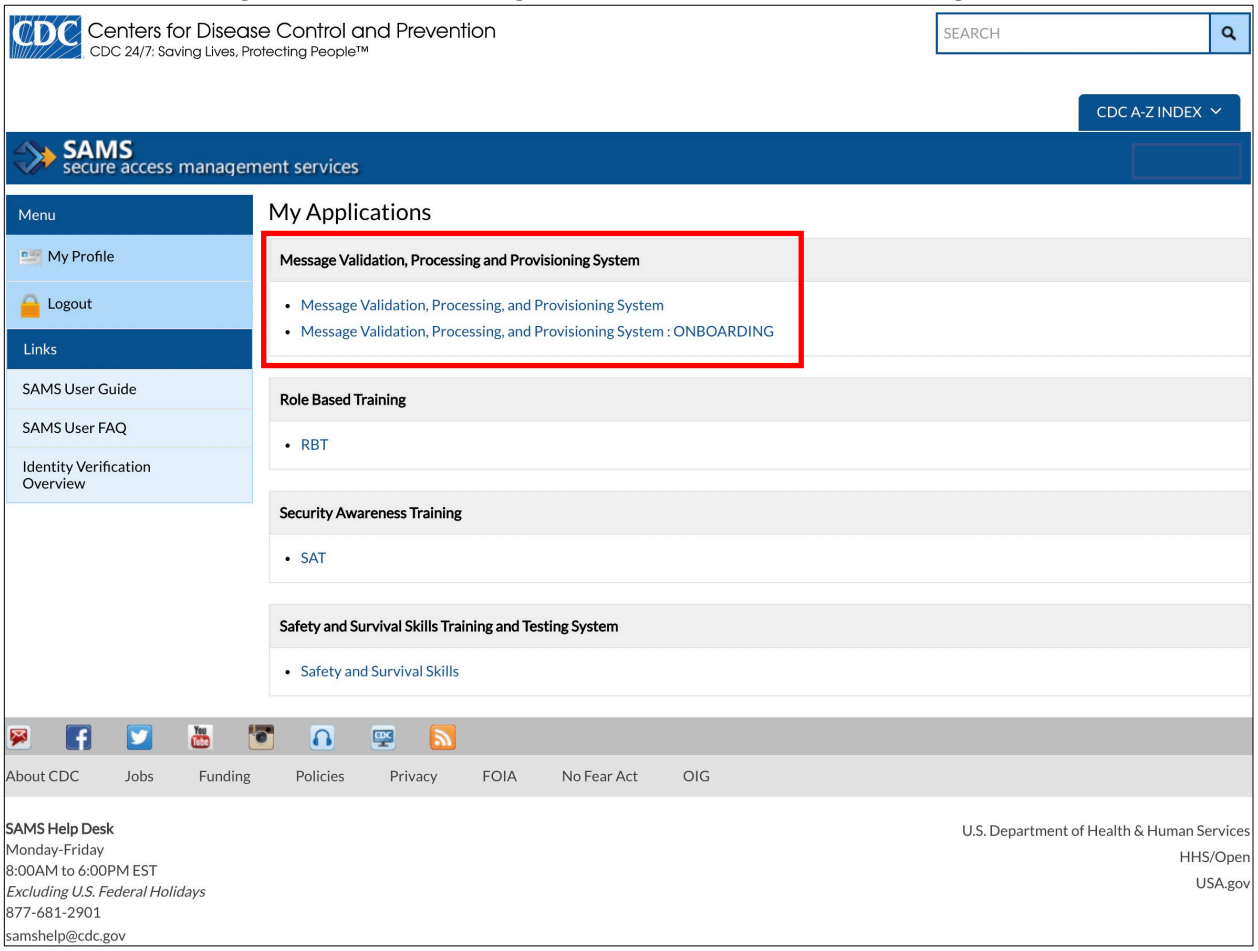
**Figure 1 – SAMS Login Page**




**Note:** To access the SAMS portal, your browser must be configured to use TLS 1.0 encryption. If your computer is not configured for TLS, or if you are unsure, please contact your local IT system administrator.

**Step 2**: In SAMS, select the MVPS link from the list of "My Applications" displayed below. The first link is for the MVPS production portal, and the second link is for the MVPS onboarding portal. Figure 2 shows access to the MVPS production and onboarding environments. Non-production MVPS systems are labeled. For example, the onboarding system is labeled in Figure 2.

**Figure 2 – SAMS User Page MVPS Production and Onboarding Links**



## Maintaining SAMS/MVPS Access

Jurisdiction users must keep their SAMS account active by:

- creating a new SAMS password at least every 60 days.
- updating any changes to contact information since initial registration, including any changes in your name, address, or email address.
- accessing their SAMS account at least once a year.

SAMS will automatically prompt users with an expired password notice to change their password at login. SAMS users should not reuse any of their last ten passwords.

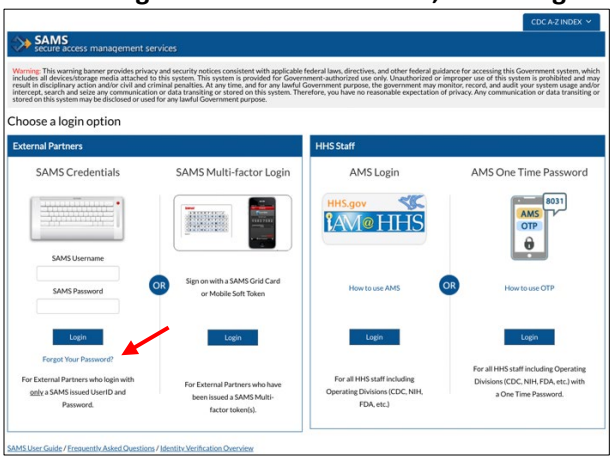
Jurisdiction users may also change their SAMS password by logging in to the SAMS portal and selecting "My Profile," and the "Change My Password" option on the "Tasks" menu (Figure 3, arrows).

**Figure 3 – How to Change Your Password in SAMS**


Please note that jurisdiction users can also use the SAMS "Tasks" menu to change their email or identity data, including their address or security questions used to verify their identity, by selecting the "Change My Email" or "Modify My Identity Data" options. Selecting the SAMS logo, at the top of the page, will return users back to the "My Applications" links.

Additionally, if a user cannot remember their SAMS password, they can select, “Forgot Your Password?” on the SAMS login screen (Figure 4, arrow).

**Figure 4 – “Forgot Your Password” Link, SAMS Login Page**

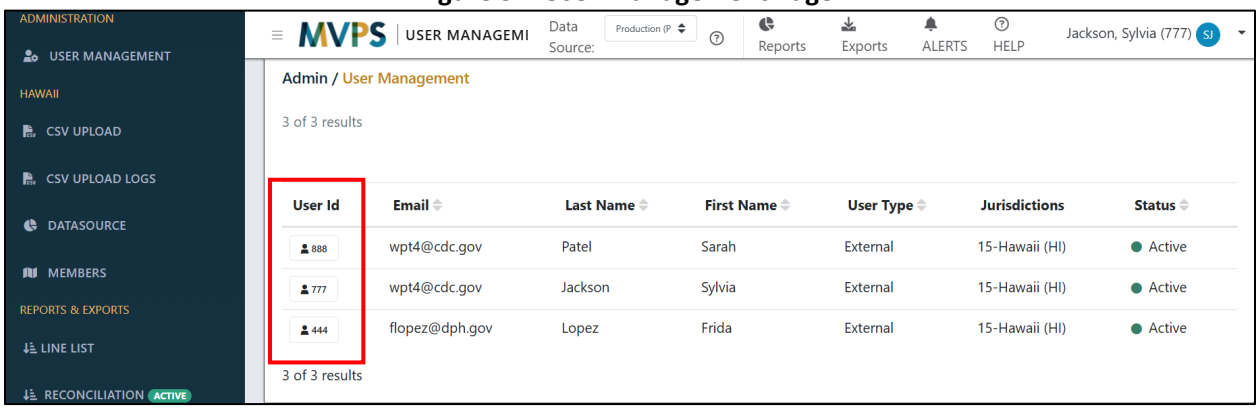



## Deactivating MVPS User Accounts

Jurisdiction users should be deactivated in the MVPS portal when they no longer need access to MVPS. When a jurisdiction user is reassigned or transferred to a different role or location in the agency, leaves the jurisdiction, or retires, a JDM should deactivate the user in the MVPS portal **within 24 hours** of the user’s departure.

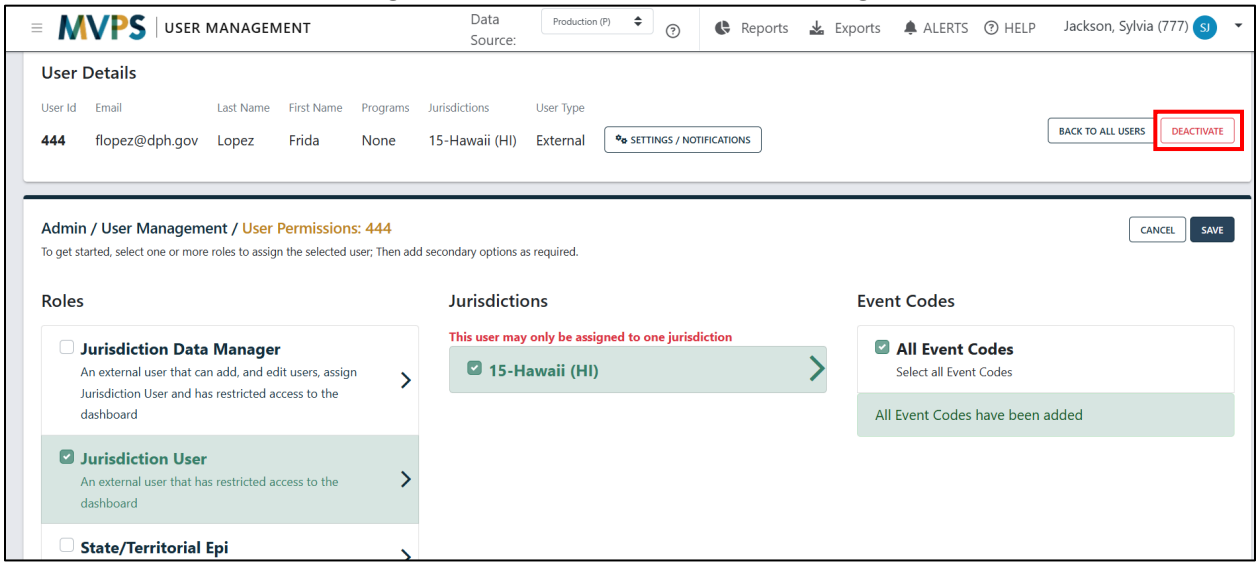
The JDM is the only Jurisdiction user role that has permission to deactivate MVPS user accounts for a particular jurisdiction. To deactivate a user account in MVPS, the JDM will first navigate to the User Management page in the portal and select the user to be deactivated by clicking on the corresponding user ID (Figure 5).

**Figure 5 – User Management Page**




Once the User Details Page opens, click the 'Deactivate' button at the upper right corner (Figure 6).

**Figure 6 – User Details – Deactivation Page**




A jurisdiction user's SAMS access will automatically expire if a jurisdiction user does not access any CDC resources, including MVPS, via SAMS within one year.

## Frequently Asked Questions

| Question | Response |
|---|---|
| **What is SAMS?** | SAMS stands for Secure Access Management Services. It is CDC's enterprise identity management and access control system for externally facing sensitive or non-public applications. |
| **What is the difference between SAMS and MVPS security?** | SAMS authenticates someone accessing a CDC system to ensure that they are who they say they are; MVPS security provides access to MVPS functionality based upon the user's role in MVPS. |
| **I have SAMS access for another CDC system. Do I need to go through the registration process again for MVPS?** | MVPS requires a Level 2 SAMS account. If the system you are currently accessing via SAMS is at a Level 2 or higher security level, then you do not need to go through the SAMS registration process again. |
| **I do not know what level of security I currently have with SAMS. How do I find out?** | Contact the SAMS Helpdesk at samshelp@cdc.gov or EDX mailbox at edx@cdc.gov. For the EDX mailbox, use the subject line, "SAMS access". |
| **I have taken a job at another jurisdiction doing this type of work. Does that affect my SAMS/MVPS access?** | A user's authorization in SAMS and MVPS is based upon their jurisdiction. When an active user in SAMS/MVPS changes jurisdictions, he or she must go through the authorization process again. |
| **I cannot see conditions and/or features that I need to view within the MVPS Portal. What should I do?** | The JDM assigns roles, conditions and features to each user when they are initially granted access to the MVPS Portal. Submit a request to your JDM to be able to view the new conditions/features. You can find a list of your jurisdiction's JDMs using the 'Members' feature found in the left side menu of the MVPS portal. |

| Question | Response |
|---|---|
| **I have a new position with my jurisdiction and do not need access to MVPS any longer, but I still need to keep my SAMS access for other CDC applications. Who do I notify?** | Notify your JDM. The JDM should deactivate your account in the MVPS portal. (A user will retain SAMS registration status but will no longer have access to the MVPS link on the SAMS landing page.) |
| **My name has changed, so I want to change my name in SAMS and MVPS. What should I do?** | Users can update some of their SAMS account information by selecting "My Profile" in SAMS, and then selecting "Change my Email" or "Modify My Identity Data" on the SAMS "Tasks" menu. If you need assistance, contact the SAMS Helpdesk at samshelp@cdc.gov or EDX mailbox at edx@cdc.gov. For the EDX mailbox, use the subject line, "SAMS access". |

If you have questions or need further assistance with obtaining MVPS Access or with your SAMS account, please send an email to the EDX mailbox at edx@cdc.gov with the following subject lines:

- MVPS New User request: "MVPS new user"
- General MVPS access inquiry: "MVPS access"
- General SAMS related inquiry: "SAMS access"

Revision History

| Version | Change Summary | Date |
|---|---|---|
| 2.0 | • Updated document header and footer to meet the new CDC Guidelines<br>• Updated Table 1 - MVPS Jurisdiction Roles – for a more user-friendly comparison between different jurisdiction roles<br>• Created a “Deactivate MVPS User Account” Section<br>• Updated the “Frequently Asked Questions” Section to include information about steps to take when jurisdiction users can’t see features within the MVPS Portal<br>• Updated the subject line to be used when sending emails to EDX mailbox to request that CDC grants them MVPS access<br>• Removed Figure 2—Default Permissions & Settings for MVPS Jurisdiction Roles | 6/24/2025 |