1.0 This guide has been designed to provide HHS users accessing SAMS with a high level overview of the ‘AMS Login’ feature.

This Guide Covered:
- 1.0 – AMS/SAMS Overview FAQs
- 2.0 – AMS Login for SAMS e-Auth Level 1 & 2 rated applications
- 3.0 – AMS Login for SAMS e-Auth Level 3 rated applications
- 4.0 – AMS Login for SAMS step-up authentication
- 5.0 – Common Issues/Error messages

Please note: This document was designed as a quick reference guide to help users login to AMS and access a SAMS protected CDC application. For more detailed information about AMS please visit https://ams.hhs.gov/amsApp/help/AMSHelp.html. For additional information about SAMS please visit https://sams.cdc.gov and login to access the ‘Links’ section on the SAMS Partner Portal.

1. AMS Overview/Introduction

What is AMS?
The Access Management System (AMS) is the primary user authentication portal used to access computer systems and software applications at the U.S. Department of Health and Human Services (HHS). Very similar to how SAMS protects applications at the CDC, AMS protects applications at HHS. Unlike SAMS however, which only protects CDC applications, AMS also protects many applications that are owned and managed by agencies and offices considered part of the HHS family.

What are the benefit of a SAMS integration with AMS?
- Removes ID proofing requirement for all employees which are part of the HHS family of agencies and offices.
- Allows SAMS Activity Administrators (AA) to easily select and assign SAMS activities to any employee within the HHS agency family. This can easily be done directly through the SAMS console.
- Allows employees to login to AMS using their HSPD-12 Access Card (PIV), AMS credentials or, if integrated, the network credentials of the employee’s agency.
- Allows SAMS to easily protect CDC applications that have only external users, only internal users, or a mixture of both populations.

**How does the SAMS integration with AMS work?**
The SAMS integration with AMS works through the setup of a trusted relationship, called Federation, between the two systems and applies only to HHS employees who need access in SAMS. When you visit a SAMS protected application SAMS will challenge you to authenticate (or prove you are who you claim to be). HHS employees will select the option to authenticate using AMS. This will take them to the AMS site (https://iam.cdc.gov) where they will successfully authenticate using one of the three options listed. After a successful authentication the trusted relationship between SAMS and AMS will redirect the user back to the SAMS protected application they need to access or the SAMS Partner Portal, based on what the user was originally attempting to access.

**What are the requirements necessary for me to use AMS for access to SAMS?**
By integrating with AMS, SAMS is no longer involved in the authentication process for HHS staff. As a result all AMS login requirements for HHS staff apply when trying to access SAMS. At a high level these rules include:

- HHS staff must be active within the HHS AMS system and have been issued an HSPD-12 PIV card that has been inducted into the HHS AMS system.
- For access to e-Auth level two rated SAMS protected applications HHS staff must access AMS using their HSPD-12 PIV card, their AMS credentials, or their OpDiv AD credentials (if setup). AMS credentials or OpDiv AD credentials can be used but not both.
- For access to e-Auth level three rated SAMS protected applications HHS staff must access AMS using their HSPD-12 PIV card. This requires the user have their PIV card in their possession and know the associated PIN. The AMS One-time-Password (OTP) option found on the SAMS home page can also be used assuming it has been setup.

*Please note:* For more information on the setup of the AMS One-Time-Password (OTP) please read the related guide found on the SAMS login page associated with the OTP login option.

**Is SAMS still protected my application now that I authenticate against AMS?**
Yes. Although it may seem that SAMS is less involved now that AMS handles the authentication of HHS staff, SAMS is still protecting your CDC applications. There is no change to how your SAMS protected application technically interact with SAMS. This is possible through the trusted
relationship called Federation that has been setup between AMS and SAMS and the existing setup between SAMS and the CDC application you need access to.

### 2.0 Using AMS to access a SAMS protected application - e-Auth Level 1 & 2

**Good To Know...**

Electronic Authentication, or e-Auth, refers to the process of establishing a confidence in an electronic user’s identity. As the e-Auth level assigned to an application increases, for example between e-Auth Level 1 and 2, the need to trust the user who is accessing the application also increases. This is important because it dictates the credentials that a user must use to login and gain access. As a general rule you can always use a high credential to access a lower e-Auth rated application. The reverse is not true.

**Minimum options to authenticate and access an e-Auth Level 1 or 2 rated SAMS protected application via AMS are:**

- AMS credentials (username/password)
- OpDiv Active Directory (AD) credentials (if configured)

1. Visit SAMS at https://sams.cdc.gov or go directly to your application using the published application specific URL. Regardless of the option you use, the SAMS main login page will be displayed.
2. As an employee of HHS or one of its agencies (for example the CDC) select the AMS Login option under the heading of HHS Staff.

Please note: For more information on the setup and use of the AMS One-Time-Password (OTP) option please read the related guide found on the SAMS login page associated with the OTP login.

3. The AMS login page will be displayed with three options available for use.
4. To access a SAMS e-Auth level 1 or 2 rated application you must use, at a minimum, the middle (Network Credentials) or right (AMS credentials) login option.

Please Note: The network credentials option must be setup for your Agency in order use. See the ‘applies to’ note to see if your Agency is listed.

5. Follow the on screen AMS login procedures to authenticate using your network credentials or AMS credentials. Following a successful AMS authentication you will be seamlessly passed to your SAMS protected application or the SAMS Partner Portal.

Good To Know...
If you have problems authenticating to AMS or have AMS specific questions you will need to escalate to AMS for support. Click the ‘Need Help?’ option on the AMS homepage. The SAMS team and SAMS Helpdesk are unable to assist with AMS specific login issues.
1. Visit SAMS at https://sams.cdc.gov or go directly to your application using the published application specific URL. Depending on the method you will see two different login pages.

If you visit [https://sams.cdc.gov](https://sams.cdc.gov) you will see the main SAMS login page:

[Image of the main SAMS login page]

If you visit your e-Auth Level three application URL directly you will see the SAMS Level 3 login page:
2. As an employee of HHS or one of its agencies (for example the CDC) select the HHS staff option to login using your HHS PIV card. Depending on your access method you will see the following:

**Screen 1** (select PIV login on AMS screen for authentication)

**Or Screen 2** (direct authentication with no AMS login screen presented)
Please note: For more information on the setup and use of the AMS One-Time-Password (OTP) option please read the related guide found on the SAMS login page associated with the OTP login.

3. Follow the on screen AMS login procedures to authenticate using your network credentials or AMS credentials. Following a successful AMS authentication you will be seamlessly passed to your SAMS protected application or the SAMS Partner Portal.

**Good To Know...**

If you have problems authenticating to AMS or have AMS specific questions you will need to escalate to AMS for support. Click the ‘Need Help?’ option on the AMS homepage. The SAMS team and SAMS Helpdesk are unable to assist with AMS specific login issues.

### 4.0 Using the AMS Login for SAMS step-up authentication

At time, HHS staff who have already authenticated to SAMS, may be required to ‘step up’ and re-authenticate for access to applications or roles that hold a higher e-Auth level rating.

For example, if a user initially authenticated against AMS to access a SAMS e-Auth 2 rated application but later required access to an e-Auth level 3 rated application during the same visit. In this situation SAMS would force the user to re-authenticate using AMS before being allowed access to the e-Auth 3 resource.

The SAMS step-up page is shown below. This page still leverages AMS for authentication using either the PIV or OTP options.
Good To Know...

On the SAMS Partner Portal application links that require e-Auth level 3 credentials are highlighted with an astrick (*) as seen in the screenshot below. Depending on how the user logged in this might force step-up authentication when the link is selected.

5.0 Common Issues & Error Messages

Given the tight integration between SAMS and AMS it can sometime be difficult to determine which system an issue or error is related to and who’s the appropriate point-of-contact (POC).

Pages:

As a general rule escalations should target the Helpdesk associated with the application where the issue occurred. In most situations the association will be clear and the related Helpdesk (SAMS or AMS) information will be displayed.
Escalate to SAMS for issues related to the following pages:

**SAMS Level 2 Login**

---

**SAMS Level 3 Login**
Escalate to AMS for issues related to the following pages:

**AMS Login Page**

![AMS Login Page](image)

**AMS Portal Pages**

![AMS Portal Pages](image)
Errors

Examples of some common SAMS and AMS generated error messages are included below. For assistance with these errors escalate to the appropriate Helpdesk.

**SAMS Federation Error** – indicates a general issue with the technical handshake between AMS and SAMS. Escalate to the SAMS Helpdesk.

### Secure Access Management Services (SAMS)

**Federation Access Request Failure**: You have attempted to access a resource that does not exist or for which you do not have authorization. Please check your request and try again. If you feel that you have received this message in error or if you have any questions or concerns, please contact the SAMS Help Desk between the hours of 8:00 AM and 6:00 PM EST Monday through Friday (excepting U.S. Federal holidays) at the following:

Toll Free: 877-681-2901
Email: samshelc@cdc.gov

**SAMS Access Error** – indicates you are currently not allowed to access. This could be because your SAMS access hasn’t been setup yet. Escalate to the SAMS Helpdesk.

### Secure Access Management Services (SAMS)

**Access Request Failure**: You have attempted to access a resource that does not exist or for which you do not have authorization. Please check your request and try again.

If you feel that you have received this message in error or if you have any questions or concerns, please contact the SAMS Help Desk between the hours of 8:00 AM and 6:00 PM EST Monday through Friday (excepting U.S. Federal holidays) at the following:

Toll Free: 877-681-2901
Email: samshelp@cdc.gov
SAMS Login Error – indicates you attempted to login to SAMS when, as a HHS staff member, you must authenticate using AMS. Retry authentication using the option labeled ‘HHS Staff’.
AMS Authentication Error – indicates an issue with your login credentials. Retry login. Escalate to AMS if required.

AMS Account Locked Error – indicates an issue with your login credentials. Following the Note 1 and Note 2 instructions or escalate to AMS if required.

For more information or assistance, please contact the SAMS Help Desk between the hours of 8:00 AM and 6:00 PM EST Monday through Friday (excluding U.S. Federal holidays) at the following:

Toll Free: 1-877-681-2901
Email: samshelp@cdc.gov