

CMS Issuer Technical Workgroup

- *Housekeeping*
- *Open Enrollment 2017 Update*
 - *Final Day of OE 2017*
 - *Reminder to Direct Enrollment Partners on TLS 1.2 Upgrade by Feb. 17t*

January 31, 2017

Troubleshooting access to CMSzONE

REGISTRATION, PASSWORD RESETS, & FORGOTTEN PASSWORDS

- **New Users:** Registration & community approval are typically completed in 1-3 business days, if not sooner.

If you are unable to access zONE, and/or the web-broker community after 3 business days you may email a follow up request to the helpdesk & the web-broker support team (addresses below) for an update. Please include any provided ticket numbers & applicable context for reference.

- **Existing zONE Users :** Password resets are also typically completed in 1-3 business days, if not sooner.

If your request is not completed after 3 business days, you may email a follow up request to the helpdesk & the web-broker support team (addresses below) for an update. Please include any provided ticket numbers & applicable context for reference.

ALL OTHER CMSzONE ACCESS ISSUES

Prerequisite Details

- Capture screenshots of any errors received so our teams can troubleshoot

☐ PC = Ctrl + PrtScn to capture, Ctrl + V to paste / Mac = Command+Shift+4 to capture & send to a desktop file

Email

- Provide screenshots and applicable prerequisite information above, in an email body, as follows:

- ❖ With the subject line: "zONE Access Issues"
- ❖ To: CMS_FEPS@cms.hhs.gov

Follow-Up Cc: or Bcc: WebBroker@cms.hhs.gov

- If the issue is not resolved within 3 business days, you may email a follow up request:

- ❖ With the subject line: "zONE Access Issues : 3+day follow up"
- ❖ To: CMS_FEPS@cms.hhs.gov & WebBroker@cms.hhs.gov
- ❖ Include (where possible) explanation message, screenshots, ticket #(s) received, and number of days outstanding

Reminder: Supported Browser Versions

- ✓ Internet Explorer Version 9.0
- ✓ Internet Explore Version 10.0
- ✓ Google Chrome
- ✓ Safari

Access to CMSzONE & the Private Web-broker Community

User Access Quick Guide

A copy of the comprehensive User Access Quick Guide is posted on zONE @:

<https://zone.cms.gov/document/zone-access-troubleshooting> (pre-log in required to access zONE links)

Three audiences:

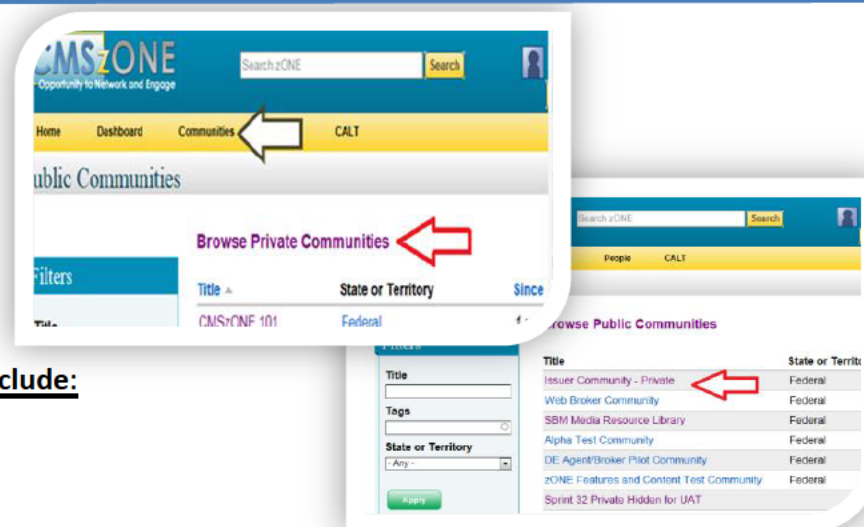
1. **New Users** (new to zONE & EIDM)
2. **Existing EIDM Users** (new user to zONE)
3. **Existing zONE Users** (unable to log-in since the EIDM transition)

EIDM Registration Process: (Pre-requisite to CMSzONE Access)

1. Register for access at EIDM Enterprise Portal Here: <https://portal.cms.gov/>
2. Log in with your EIDM credentials and click on "Request Access Now"
3. Click on "Request New Access" and choose CMSzONE

CMSzONE Private Web-broker Community Access: (After being granted EIDM access)

1. Log into zONE; click on the Communities tab
2. Click Browse Private Communities
3. Click Web-broker Community – Private
4. Click Join Community
5. Provide explanation of why you need access to this community; Include:
 - name and contact information
 - web-broker POC contacts
 - specific work for web-broker (i.e. access web-broker resources, etc.)



Open Enrollment 2017 Update

- 
- ✓ Highlights for Production Week 14 (OE Ending Tonight)
 - ✓ Direct Enrollment Partners: Reminder on TLS 1.2 to Complete by Feb.17th

January 31, 2017



Open Enrollment 2017: Production Highlights for Week 14

- **Open Enrollment Ends Tonight:** OE closes at 11:59 Pacific Time (to accommodate western time zones.) There are no new critical systems issues at this time. Direct Enrollment functionality will continue to work after the close of OE. Thanks to all the issuers, web brokers and operations partners for making OE a success this year!
- **Direct Enrollment Partners! Remember You Must Upgrade to TLS 1.2 Action Needed by Friday, Feb. 17th:** A repeat reminder: Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). Since the summer we have announced we have moved to TLS 1.2; all of the data partner connections to the Hub that are not currently connected via TLS 1.2 will need to migrate from their current version. All issuers /web brokers/ partners using the Hub should make sure they have upgraded to using TLS 1.2. See the following slides and please make sure this occurs by **Friday, February 17th.**
- **1095-A IOT New 'Shared Secret' Password Process starting March 1, 2017:** See following slides from the 1095-A Issuer Outreach Team (IOT) detailing the new enhanced password protection process starting March 1, 2017. This will replace the previous process and will be more aligned with CMS security standards.

Reminder on TLS 1.2 Upgrade for the Hub

(Repeat on the Slides We Presented Summer/November/January)

Overview

- Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are an industry standard designed to protect the privacy and data integrity of information communicated over the Internet
- The Data Services Hub (DSH) has migrated to TLS 1.2 in order to support the NIST and GAO recommendation that requires all governmental communications use either Transport Layer Security (TLS) v1.1 or TLSv1.2
- The Hub has enabled support for TLS 1.0 and 1.2 in the Implementation and Production regions
- The Hub will continue supporting TLS 1.0 and 1.2 concurrently to allow all Partners to verify successful connectivity using TLSv1.2

DE Partner Readiness

- Direct Enrollments partners need to ensure that they are able to support TLS 1.2 version by their existing infrastructure
- As part of the upgrade the Hub will not be introducing any new endpoint/ports.
- The Hub security policy requires that all partner certificates have:
 - Signature algorithm of SHA-2 or greater
 - Key length of at least 1024 bits

TLS 1.2 Timeline & Testing Requirements:

Please make sure you have migrated by Feb. 17th!

- Partners can test TLS 1.2 connectivity with the Hub at any time.
- Our goal remains to successfully migrate the majority all partners to TLS 1.2 before the close of Open Enrollment.
- Hub will stop supporting TLS versions below 1.2 for all CMS Interfaces on **Friday, February 17th**. (Previously we communicated end of January.)
- DE Partners can use the H74 Hub Connectivity service to ensure that they are able to connect to HUB: <https://zone.cms.gov/document/hub-connectivity-service>
- Partners MUST ensure that they are able to connect to the IMP1A environment via TLS 1.2 before moving to Production.
- Upon successful connectivity to each environment, Partner will send an email to dsh.support@qssinc.com with the following:
 - **Subject Line: “TLS 1.2 Testing Completion– [HUB Partner ID]”**
 - **Environment**
 - **Request Timestamp**
- CMS will be monitoring the site traffic to validate which version of TLS Partners are using.
- Any issues identified during testing should be sent via email to DSH.Support@qssinc.com. Copy the CMS Helpdesk CMS_FEPS@cms.hhs.gov to create a ticket. Please include the subject **“TLS 1.2 Testing Issue – [HUB Partner ID]”** with details on timestamp, environment, and screenshot/details of any errors you encounter.