



USAccess Blue Top Newsletter

December 1, 2016

Volume 9, Issue 22

- [Upcoming Meetings and Trainings](#)
- [Issue with coil card stock being used; card batching halted on November 29, 2016](#)
- [Mandatory PIV card login for roleholder portals](#)
- [Service Enhancements](#)
- [Security Tip](#)

Upcoming Meetings and Trainings

Footprint Management Working Group

- **Tuesday, December 6, 2016, 9:30am - 12:00pm**
- Location: <https://meet.gsa.gov/fmwg/>, passcode: footprint
- Conference Line: [1-866-928-2008](tel:1-866-928-2008), passcode: 474534

Registrar Refresher Training

- **Thursday, December 8, 2016, 2:30pm - 3:30pm**
- Location: <https://meet.gsa.gov/r1njwtxf41/>
- Conference Line: [1-888-455-1864](tel:1-888-455-1864) passcode: 3611044

Customer Advisory Board (CAB)

- **Tuesday, January 10, 2017, 9:30am - 12:00pm**
- Location: GSA Central Office 1800 F Street, NW, Room: 3046

User Group Meeting

- **Tuesday, January 17, 2016, 9:00am - 12:00pm**
- Location: GSA Central Office 1800 F Street, NW, Room: 3042
- Conference Line: [1-866-556-0154](tel:1-866-556-0154), passcode: 2132069

Registrar Classroom Training

- **December 7-8, January 11-12, February 15-16, March 15-16**
- Location: HPE, Chantilly
- Contact [Jim Schoening](#) for information

Issue with coil card stock being used; card batching halted on November 29, 2016

The MSO sent emails to Agency leads on November 29 and November 30 regarding an issue where USAccess PIV credentials printed at our central card print manufacturer were inadvertently printed on the tri-interface/coil card stock. Printing on this coil cardstock was an error made by our centralized card print vendor and impacted all cards centrally batched and printed from November 20-November 29. (Roughly 4,000 cards.)

We turned off batching for most of the day on November 29 until a fix could be applied by our printing vendor. The issue was fixed late in the day on Tuesday, November 29, and we resumed batching at 3AM Eastern on Wednesday, November 30.

Agencies with cards printed on coil cardstock received a list of card serial numbers so they can assess impact and determine if reprints are needed. This is being done on a case by case basis and deemed necessary only if the coil card does not work properly within an Agency's IT infrastructure. Most Agency PACS systems can read the coil cards (as they were actively printed until January 2016) so the MSO expects the need for reprint requests to be minimal.

However, if your agency determines a need for a card reprint, please work through the USAccess helpdesk (USAccess.Helpdesk@hpe.com or [1-866-493-8391](tel:1-866-493-8391)) to request a reprint as there is a specific code available to the Tier 3 team to correctly issue reprints for this event.

We appreciate your patience as we work through this issue to a resolution. As always, please reach out to the MSO with any questions.

Mandatory PIV card login for roleholder portals

Currently, roleholders have a choice to use their username and password or their PIV card to get into some of the USAccess roleholder portals. **However, effective January 7-9, 2017, all USAccess roleholder portals will require a PIV login.** This date coincides with scheduled mandatory maintenance.

The following portals already require a PIV login:

- Assured Identity (Enrollment and Attended/Unattended Activation)
- PCA (Activation and Local Print)
- Credential Inventory Tool
- Site Manager

The following portals will be affected by the change:

- Assured Identity (Sponsorship, Security Officer, Adjudication)
- Report Viewer
- TRACKS
- Role Administration
- Self Service Password Reset

MSO will continue to publicize this requirement in the time leading up to this change.

Service Enhancements

Changes/updates since last Blue Top

- Entrust maintenance completed as scheduled on November 13. The 2nd Entrust maintenance (OCSP migration to new servers) that was initially performed on November 17 was rolled back on the evening of Monday, November 21. The MSO sent out communications to Agencies once Entrust notified them of their plans on the morning of the 21st. This rollback rectified several issues reported by Agencies within their IT infrastructures as well as from several fixed workstation operators who experienced slowness when logging on to their workstations.
- USAccess Software Release 10 went in to production on November 19 as planned. A release notice is posted on the ALP.

Planned changes

For any maintenance downtime periods, please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.

- Maintenance is planned for the USAccess service on Saturday, December 3. The USAccess service will be unavailable from 8:00am Saturday through the afternoon of Sunday, December 4.

Security Tip

Protecting Your Government Owned Equipment and Personally Identifiable Information

Agency workplaces and telework provide great flexibility in how we accomplish our jobs. That flexibility requires each of us to be diligent in how we properly handle and secure our Government owned equipment and Personally Identifiable Information (PII).

Below are some tips that each of you should make part of your daily routine whether you are physically in the office or working remotely. Please take a moment to review them carefully.

Top Tips for Keeping PII and Government Owned Equipment Secure in a Flexible Workplace:

- Lock your computer when you step away
- Secure your agency issued laptop and other mobile devices
- Protect and secure documents when you send them to the printer
- Don't leave documents that have PII out on your desk when you're not there
- Lock all PII documents in a secure storage unit when you're not actively working with them
- Encrypt all PII being sent outside of your agency network

Every federal employee has a responsibility to make sure their Government owned equipment and sensitive or Personally Identifiable Information is secured.

Contact Sharon Meng (Sharon.Meng@gsa.gov) to be added to USAccess distribution lists.

STAY CONNECTED:

