



Blue Top Newsletter

USACCESS Program

Upcoming Meetings and Training

| Meeting/Training | Date & Time (EST) | Location | Dial-In Info |
|------------------------------|---------------------------------------|----------------------|--|
| CAB | Wed, July 12 9:30 to 12:00 | TBD | No telecon provided |
| Registrar Refresher Training | Thu, July 14 2:30 to 3:30 | Telecon/Webinar | 888-455-1864 Passcode: 3611044 |
| Registrar Classroom Training | Wed and Thu Jun 15-16 Jul 20-21 | HPE Chantilly, VA | Contact Jim Schoening for information or to Register |

Light Installers v4.0.3 released soon; USAccess Software Release 9.10 and 10.0

An expiring jar file and recent CMS software changes require updates to both the light and fixed stations. The three scheduled release packages are described below, as well as the possible impacts to station operators if these updates are not made timely.

- **Light Installers v4.0.3 - prior to June 19**
 - The Light Installers v4.0.3 will be posted on the USAccess SFTP site within the coming week. An email will be sent to Agency Leads when it's available for download. A release notice for Light Installers v4.0.3 is posted on the ALP. An .msi file that contains the new ActiveX controls will also be made available at the same time as v4.0.3 to those who use their systems for desktop rekey. The package will be called USAccess Desktop Rekey June 2016.zip.
- **USAccess Software Release 9.10, and 10.0 - June 25**
 - USAccess Software Releases v9.10 and 10.0 are tentatively scheduled for Saturday, June 25. A spreadsheet detailing changes included in this release as well as 9.10 release notes are posted to the ALP

Special Points of Note:

Now found on www.fedidcard.gov:

- > Service Order Requests and Test Card Orders
- > Role Holder Web Based Training Registration
- > Deployment Activities and USAccess Center Status Alerts
- > Contact Sharon Meng (Sharon.Meng@gsa.gov) to be added to USAccess distribution lists.
- > Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up

Inside this issue:

| | |
|--------------------------------|-----|
| Meetings and Training Calendar | 1 |
| Spotlight Articles | 1-3 |
| Service Enhancements | 4 |
| Security Tip | 4 |

Fixed workstations will be updated using our automated means so no additional action is needed by agencies to get the fixed machines updated. A reminder to keep fixed machines powered on will be posted to TRACKS.

Contents of Light Installers v4.0.3

- **Updated Jar file:** A Jar file used on Light and Fixed Activation stations is **expiring on June 19** (a Sunday). Fixed Activation workstations will be updated with the Jar file before 6/19, but Agencies will need to download the Light Installers v4.0.3 file from the SFTP and deploy to their machines. If not updated and it expires, the Acknowledgement Page that follows any activation or update activity won't populate correctly, and role holders will have issues using the Credential Inventory Tool and the self-service password reset portal when accessing it from the Light system. **Activations can still occur** but Activators should use a fixed machine to check in cards via CIT or to use the Self Service Reset Portal until the machine is updated to v4.0.3. (See workarounds below.) These issues will continue until the Light system is updated to v4.0.3.
- **New ActiveX controls:** USAccess Software Release 9.10 includes a CMS hotfix that has new ActiveX controls. **This release is tentatively scheduled for June 25**. These ActiveX files must be on Light machines once the CMS hotfix goes in, or Activators can't complete card activations or updates using their Light machines. If the system is not updated, then Activators will see issues with the system detecting card readers and photos displaying properly.
- **Java 8 Update 91:** Per our policy to periodically update Java, Light Installers v4.0.3 contains an update to Java 8 Update 91. Light machines that were updated to v4.0.1 currently run Java 8 Update 73.

Workarounds until upgrade to v4.0.3

- **USE PCA:** PCA is unaffected by both the Jar file expiration and the CMS hotfix ActiveX controls. Activators can use PCA to activate credentials until they update to v4.0.3. NOTE: CIT will still be impacted so please see workaround below for CIT.
- **If PCA is not an option:**
 - **Acknowledgement page issues:** Activators should either close the page/not digitally sign it (but print it out for an Applicant to manually sign), or access the page using a Fixed Activation machine. (Fixed will work because we can push the update automatically before June 19.)

- CIT and Self Service Reset Portal issues: Activators can either contact Applicants to come pick up their cards or use a Fixed system to check in the cards and send “Card Ready for Pick up” emails until their Light systems are updated. They can also use either a Fixed machine or another machine with Internet access to use the password reset portal. (Fixed will work because we’ll push the update automatically before June 19.)

For more information please see the drafts of Light Installers v4.0.3 Release Notice as well as a Release 9.10 release notice and a Release 10 spreadsheet detailing changes included in this release as well as updates to documentation on the Agency Lead Portal.

We realize that updating Light machines in the field is no small feat and requires considerable time and effort from you and your IT teams. We hope that using PCA will alleviate much of the frustration you might otherwise experience until you are able to upgrade your Light systems to v4.0.3.

Mandatory PIV card login for roleholder portals

At this time some role holders have a choice to use their username and password or their PIV card to get into the USAccess role holder portals. However, as an effort to enhance security, as of January 1, 2017, all USAccess role holder portals will require PIV login. A list of the portals affected are as follows:

- Sponsorship
- Enrollment
- Adjudication
- Attended and Unattended Activation
- Report Viewer
- Credential Inventory Tool
- Site Manager
- Security Officer
- Print Operator
- TRACKS

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

All roleholder training and job aids on GoLearn Portal

All USAccess Job Aids and refresher trainings are now available on the GoLearn training portal. Roleholders can view and download them from the portal and do not have to have an ALP account to access them.

You can access the trainings and job aids at piv.golearnportal.org. To get an account use your work email address and the registration password of 12345678 to create an account. Each role is listed so users can click on their role and get the available job aid.

Service Enhancements

Changes/updates since last Blue Top

- Completed maintenance as scheduled on Friday, June 4.
- Added OPAC Combination for GSA and CSB

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.

- **June 25** Maintenance is tentatively scheduled for Saturday, June 25 as part of the work of pushing USAccess Software Release 9.10 and 10.0 to production. The USAccess service and portals will be unavailable for most of the day. Please see the article above for more information on these releases.

Security Tip

Security Incident Responses

This week's security tip covers how to respond to security incidents involving USAccess. Please follow these steps to report an incident:

1. Contact your System ISSO or Agency ISSM within one (1) hour of the incident.
2. Your Agency ISSO or ISSM should contact the MSO Program Office
3. At a minimum, GSA will need the following information:
 - A brief description of the incident;
 - A description of the types of Personally Identifiable Information (PII) involved (e.g. full name, Social Security Number, date of birth, home address, account number, etc.);
 - Date(s) of the breach;
 - How it was discovered;
 - Encryption or protected status of the PII if known; and
 - The name of the person(s) that the GSA MSO should contact for more information (contact information should include a telephone number, e-mail address, and street address if available).
4. The GSA Security Team will work with your Agency Security Office to:
 - Determine what steps the Agency and individual should take to protect himself/herself from potential harm;
 - Determine what steps GSA will take to investigate the breach, mitigate losses, and to protect against any further breaches; and
 - Assign an Impact Level for the incident and determine the potential impact on GSA, the Agency or the potential for identity theft of the individual Three levels may be assigned.

The impact level assigned by GSA to the information breached will determine when and how the incident will be addressed. Higher Impact Levels may require additional information from you and your Security office. GSA Impact Levels are defined as:

Low – the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organization operations, organizational assets or to individuals.

Moderate – the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations or to individuals.

High – the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic effect on organizational operations, organizational assets, or to individuals.

Customer Loyalty Survey

As a reminder to all agencies, you should have received an email containing a link to our annual Customer Loyalty survey. The purpose of this survey is to help the General Services Administration Federal Acquisition Service (GSA FAS) monitor customer satisfaction and loyalty. Your feedback will identify ways we can enhance and improve your customer experience using the USAccess Program.

Providing information is voluntary. Your responses will be completely confidential and will only be released in group summaries and will not contain personally identifiable data.

Please take a few moments to fill it out before the survey closes on June 21st. We look forward to your feedback so that we may better serve you.