



USACCESS Program

Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
User Group	Tue, Jul 21 9:00 to 12:00	GSA Central Office 1800F St. NW Conference Rm. 6044	888-455-1864 Passcode: 5887966
CAB	Thu, Aug 6 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
Registrar Refresher Training	Thu, Aug 13 2:30 to 3:30	Telecon	888-455-1864 Passcode: 3611044
Registrar Classroom Training	Wed and Thu Jul 15-16 Aug 12-13 Sep 16-17	HP Chantilly, VA	Contact Jim Schoening for information or to Register

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 Steve Sill (Stephen.sill@gsa.gov) to be added to User Group (UG) distribution list.
- > Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up

USAccess and Java

The MSO has been notified of agency concerns about Java as it is currently used in USAccess. We decided to address this issue prior to the July User Group due to concerns that were surfaced last week.

Below is a summary of our plan to mitigate concerns brought up at the NCE. We have outlined where Java currently is used with our Fixed and Light workstations and how we plan to address.

Where Java is currently utilized on Fixed and Light workstations

Java is currently utilized on Fixed and Light workstations within the Acknowledgment Page applet, the Credential Inventory Tool (CIT) and the Self Service Password Reset Portal (used by Applicants to have a temporary password sent to them to if they don't know their PIN/ need to reset it to complete a card update or activation using Unattended Activation.) The CMS is currently configured with Java disabled as it relies on ActiveX (NOTE: IE is the only browser supported with this setting.) So other than Acknowledgment Page, CIT and the Self Service Password Portal, Java is not used anywhere else on Fixed and Light machines.

Inside this issue:

Meetings and Training Calendar	1
Spotlight Articles	1-4
Service Enhancements	4-5
Security Tip	5

USAccess and Java continued

Fixed Workstation Plan—Migrate 8/1/15

As presented in the past few program review roadmaps, the Fixed workstations are currently scheduled to migrate to Java 8 as part of monthly maintenance on Aug 1. Testing will continue as scheduled, and Java 8 will be pushed to Fixed workstations on 8/1/15 barring any issues with testing. This will address DOI's concerns and help them meet their internal deadline of deploying Java 8 by August.

Light Workstation Plan—Light Installers v3.4.2 available early August

Testing began last week on upgrading to Java 8 on LA and LCS kits. Following testing, LA and LCS installation packages (both v3.4.2) will be posted on the SFTP server for Agencies to download. Barring any issues uncovered with testing, we anticipate making these new installers available in early August. If any Agencies must migrate to Java 8 before then, they can download the Java 8 installer from the vendor and install themselves on their Light kits, but do so at their own risk. The Light v3.4.2 installation packages are not mandatory, meaning if Agencies choose not to deploy, their LA and LCS kits will continue to work with current versions.

Long Term Solution—Deploy PCA

As discussed in previous meetings (including User Groups with Agencies), PCA offers many advantages, the first of which is better usability for Activators and more effective self-service options. We believe USAccess should utilize PCA as soon as possible. We feel Agencies, once properly trained on the changes to current processes, will embrace it and find it addresses many of their current concerns with the existing activation application.

We have considered accelerating the roll out of PCA instead of migrating to Java 8 to address certain immediate concerns, but realized that while PCA does not use Java, there are still other applications such as the CIT and the Self-Service Portal that are dependent on Java. Thus, PCA by itself will not address the immediate August Java vulnerability concerns, and additional development work is required to make the existing Java based applications/applets work without Java. In addition, a full field training program must be developed and executed because of the entirely new look and feel of PCA and the changes to the activation process so that our Activators and Applicants can take full advantage of PCA. As we learned with our recent Windows 7 migration project that included mandating PIV card log on, taking the time to develop solid materials and prepping our role holders is key to adoption.

USAccess and Java continued

As a result, the MSO strongly recommends that we continue with our plan to migrate to Java 8 on the fixed infrastructure as previously planned for 8/1, and focus development efforts on developing new Light installation packages to migrate our LA and LCS kits to Java 8 as soon as possible. We can then work on a plan for rolling PCA out to the field this Fall.

Naturally, we expect to address this issue further at the User Group on July 21.

Customer Loyalty Survey Reminder

You still have until **July 17** to complete this year's 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.

We look forward to your feedback so that we may better serve you.

New Agency Lead Portal URL

The URL for the Agency Lead Portal (ALP) has changed. The new URL is:
<https://usaccess-alp.gsa.gov>

The previous URL will forward you to the new URL until August 15, 2015, at which time the previous URL will no longer be active. Please take the time to update your bookmarks to the new URL.

The MSO team has notified all ALP users of this change via email and an announcement has placed on the ALP notifying users of this change.

Please let us know if you experience any issues with this change.

Distribution List Cleanup

The MSO is in the process of cleaning up our distribution lists. Next week we will be reaching out to each Agency Lead for assistance in this process. We will be asking you to review the MSO distribution list members from your agency and provide feedback. As part of the same process we will be asking you to review your agency's USAccess Financial POCs and Agency Lead Portal users. Detailed instructions will be provided in next week's email to Agency Leads.

Service Enhancements

System Changes Since Last Blue Top

- Support Migration to Encrypted SIP Web Service for SEC
- Filter older certificates from the list returned in QuerySIP
- Maintenance was successfully completed on June 27.

Planned Changes

- **Maintenance on FEDIDCARD.GOV web site, July 10-12**
The GSA MSO will be conducting maintenance on the fedidcard.gov website server beginning Friday, July 10 at 8:00PM ET and continuing through Sunday, July 12 at 6:00PM ET. Please plan for the website to be down most of the weekend.
- **Maintenance is scheduled for July 11-12**
Maintenance is scheduled for Saturday, July 11 from 6:00AM ET to Sunday, July 12 12:00PM ET. During this time, the USAccess Service and all role holder portals will be unavailable.
- **Update to GSA Online Scheduling System planned for July 15**
The vendor managing the GSA Online Scheduling System has notified us of an update to the GSA Online Scheduling System software planned for July 15. As a result of this maintenance, Internet Explorer 8 will no longer be supported for the Scheduler. We encourage Agencies to upgrade to later versions of IE when accessing the scheduling system. The fixed credentialing workstations are all operating on IE 11 as a result of the Windows 7 migration.

Security Enhancements Continued

- **Maintenance on FEDIDCARD.GOV web site, July 10-12** Entrust cert update being planned for July

The PIV Content Signing Certificate used by the system to sign card contents must be renewed in August 2015. As part of this work, our CA provider (Entrust) must also update their CA root certificate. Meetings are occurring between GSA MSO, HP and Entrust to schedule this work. Once plans are in place, an announcement will appear in the Blue Top and the next User Group meeting outlining outage times expected.

- **Maintenance scheduled for July 17-19**

Maintenance is scheduled beginning at approximately 7:00PM ET on July 17 and continuing through the weekend. During this time, the USAccess Service will be unavailable. Please plan for it to be unavailable for most of the weekend.

- **Maintenance schedule for August 1**

Maintenance is scheduled for Saturday, August 1. During this time, the USAccess Service will be unavailable. Please plan for it to be unavailable for most of the day.

Security Tip

Handling Logical and Physical Access Problems

Physical Access Control Systems or PACS, are systems that manage physical access into building and other control areas. For example, the system that is used to swipe your card to enter a secured room or that scans your credential before you enter a Federal building, is a PACS. Logical Access Control Systems or LACS, are systems that manage network and computer access. For example, the system that allows you to insert your credential into your computer and enter your PIN in order to log into your computer, is a LACS. If a cardholder comes to your activation station reporting trouble with physical or logical access using their credential, please take the following steps:

First, the Activator should check the credential status using the activation station, to see that the credential is active and has no updates pending. This can be done using Attended or Unattended Activation.

If the credential is active and up to date, refer the credential holder back to their local IT team or building's security office to have their credential checked for logical or physical access issues. Oftentimes access issues related to a functional credential are due to account management errors on the PACS and LACS administration side.