



USACCESS Program

# Blue Top Newsletter

## Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
CAB	Thu, Sep 10 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
Registrar Refresher Training	Thu, Sep 10 2:30 to 3:30	Telecon	888-455-1864 Passcode: 3611044
User Group	Tue, Sep 15 9:00 to 12:00  August UG has been cancelled	GSA Central Office 1800F St. NW Conference Rm 6044	888-455-1864 Passcode: 5887966
Registrar Classroom Training	Wed and Thu Sep 16-17	HP Chantilly, VA	Contact Jim Schoening for information or to Register

Special Points of Note:

Now found on  
[www.fedidcard.gov](http://www.fedidcard.gov):

- > Service Order Requests and Test Card Orders
- > Role Holder Web Based Training Registration
- > Deployment Activities and USAccess Center Status Alerts
- > Contact Ken Bandy ([Kenneth.bandy@gsa.gov](mailto:Kenneth.bandy@gsa.gov)) to be added to User Group (UG) distribution list.
- > Contact Jim Schoening ([jim.schoening@gsa.gov](mailto:jim.schoening@gsa.gov)) for Registrar Classroom Training sign up

## UPN Password Resets Needed on Fixed Workstations

As part of the project this past Spring/Summer to replace Windows XP USAccess fixed enrollment and activation workstations with a Windows 7 machine, all Registrars and Activators were asked to learn their UPN and use it to reset the UPN password (not to be confused with the credential PIN.) This was necessary to enable Registrars and Activators to use their PIV card to log on to their fixed credentialing machines and as a means of **reducing incidents of shared role holder credentials.**

These UPN passwords are set to expire every 90 days, and therefore the first set of passwords must be reset. Registrars and Activators won't be prompted ahead of the expiration date to reset the password. Rather, they will see a "your password has expired" message when attempting to log in to their fixed enrollment or activation machine.

Registrars and Activators who see this password expired message during workstation log on should follow the steps outlined in a document

### Inside this issue:

Meetings and Training Calendar	1
Spotlight Articles	1-3
Service Enhancements	3-4
Security Tip	5

that was posted on TRACKS in the Training section of the portal. The document is called *Guidance on resetting UPN Password on Fixed Workstations*. This document was also posted as an advisory on the home page of TRACKS on August 6. It contains instructions similar to the steps Registrars and Activators completed to reset their UPN passwords during the Windows 7 workstation replacement process.

The USAccess Help Desk is familiar with this document and can assist callers if they have issues resetting their UPN password. Please share the guide with your Registrars and Activators so they are familiar with how to reset their UPN password.

### **Integrated Project Team (IPT) Participation**

The MSO and GSA Management are requesting your participation in the USAccess Core Services Integrated Project Team (IPT). Please see information below regarding participation, including contractor participation, and expected time commitments.

All IPT nominations and Non-Disclosure Agreements (NDA) are needed no later than close of business (COB), **Friday, August 14, 2015**.

Participation Requirements for the USAccess Core Services IPT:

- All IPT participants, including Federal employees and contractors, must sign the NDA, which is specific to this procurement prior to attending the first IPT meeting. The NDA was sent to agency leads on August 4. Please contact the MSO if you require another copy.
- Agencies may nominate contractors to participate in the IPT, but must provide the names of the companies they represent, work for, or have a working relationship with, that are associated with the work being performed for USAccess customers.
- The companies that are represented as noted above shall be barred from submitting proposals on any piece of the USAccess Core Services procurement effort, including any prime/sub-contractor arrangements.
- The IPT shall meet twice a month. Members can attend in person (conference room at GSA) or via teleconference/webinar. The meetings are expected to be scheduled for 2 hours in duration.
- The IPT may determine it needs to meet more or less than twice a month.
- IPT working groups will be established and meet as needed.

## **Final Reminder—New Agency Lead Portal URL**

The ALP URL has changed. The new URL is: <https://usaccess-alp.gsa.gov>. The previous URL will stop forwarding to the new URL after August 15, 2015. Please take the time to update your bookmarks to the new URL.

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

## **Service Enhancements**

### **System Changes Since Last Blue Top**

- **Activation outage on Friday, July 24 due to Entrust issue.**  
All USAccess activations could not complete for approximately 3.5 hours on Friday morning due to an issue with Entrust, our CA provider. The cause was an update that Entrust pushed out the night before. We engaged Entrust early on in the process, and when they began troubleshooting the issue, they discovered the problem and pushed a fix to their service. The USAccess support team then restarted the services on our side, which allowed activation activities to complete. We posted advisories on TRACKS, [www.fedidcard.gov](http://www.fedidcard.gov) and sent an email to Agency Leads. We apologize for any inconvenience.
- **USAccess Software Release 9.6.7 and maintenance completed as scheduled on Saturday, August 1. A release notice is posted on the Agency Lead Portal.**  
This release included an update to the PIV Card Required field in the Sponsorship Portal to make it more intuitive for a Sponsor to indicate whether an Applicant should have a card printed. The *PIV Card Required* field was renamed *Credential Option* with a pull-down option to select:
  - *PIV=A* card should be printed for the Applicant.
  - *NONE*=The Applicant should not have a card printed.The field defaults to *PIV*. A release notice is posted on the Agency Lead Portal.
- **Renewed Entrust CA and root CA certificates and posted new trust chain on Thursday, 7/30.**  
Entrust updated their CA root certificate on July 30 and a new trust chain that must be incorporated in to Agency infrastructures was posted on the SFTP server (and also available from the Entrust site) the same evening. Agencies were briefed during the July User Group meeting and several emails sent to Agency Leads. Agencies must update any computer system where access certificates are being validated (e.g.; workstations, servers, VPNs, PAC systems, etc.) and use these CA certificates to validate.

**NOTE:** Any certificates issued after the Entrust root CA rekey require this new trust chain to be validated. If the trust chain is not imported, new cards or cards receiving updates under the new CA certificates may not be usable for PIV card log on, etc.

Planned Changes

**Maintenance will occur for the next three weekends and involve downtime of the USAccess service. Please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.**

- **Maintenance scheduled for this Saturday, August 15 from 6am-10pm Eastern**  
A TRACKS advisory will be posted on Thursday reminding Registrars and Activators to leave their workstations powered on for the weekend and that enrollments and activations cannot be completed during this time. An advisory will also be posted and an email sent from [www.fedidcard.gov](http://www.fedidcard.gov).
- **Maintenance \*tentatively\* schedule for Saturday, August 22 from 6am-10pm Eastern**  
This is for backend CMS server maintenance to upgrade to Windows 2012. A TRACKS advisory will be posted notifying Registrars and Activators that enrollments and activations cannot be completed during this time and an advisory will also be posted and an email sent from [www.fedidcard.gov](http://www.fedidcard.gov). If the schedule changes for this release, we will send an updated email to Agency Leads with the new schedule for this maintenance.
- **Maintenance scheduled for Saturday, August 29 from 6am-10pm Eastern and \*potential\* intermittent issues on Sunday, August 30 all day**  
The Saturday outage period is for standard August maintenance. A TRACKS advisory will be posted notifying Registrars and Activators that enrollments and activations cannot be completed on Saturday, August 29 from 6am-10pm Eastern, and an advisory will also be posted and an email sent from [www.fedidcard.gov](http://www.fedidcard.gov).  
  
On Sunday, August 30, our regular security scans are occurring, so role holders may experience delays during the scanning period. TRACKS and [www.fedidcard.gov](http://www.fedidcard.gov) advisories will be posted stating role holders may experience intermittent issues.
- **Update on Light installers v3.4.2 that update machines to Java 8**  
The Light Installers v3.4.2 can be used to upgrade a Light Activation (LA) or Light Credentialing Solution (LCS) machine to Java 8. These installers will be posted on the SFTP server on Saturday, August 15. The MSO will send an email when they are posted. While these installers are not mandatory updates (i.e.; LA and LCS workstations will still operate if not upgraded from v3.4 to v3.4.2), it is **strongly recommended** that Agencies update their workstations. A release notice is posted on the Agency Lead Portal.

NOTE: Fixed credentialing workstations were already updated to Java 8 using our automated update system and no further action is needed by Agencies.

## 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
  - 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.