



USAccess Blue Top Newsletter

July 28, 2016

Volume 9, Issue 14

- [Upcoming Meetings and Trainings](#)
- [Delay in Release date for 9.10 and 10](#)
- [Customer Access Control List Update](#)
- [Entrust ATO Status](#)
- [Reminder to Review the Registrar Daily Checklist](#)
- [Remember to subscribe to the Blue Top Newsletter](#)
- [Service Enhancements](#)
- [Security Tip](#)

Upcoming Meetings and Trainings

Customer Advisory Board (CAB)

- **Tuesday, August 2, 2016, 9:30am - 12:00pm**
- Location: GSA Central Office 1800 F St., NW Room 4143

Registrar Refresher Training

- **Thursday, August 11, 2016, 2:30pm - 3:30pm**
- Location: <https://meet.gsa.gov/r1njwttxf41/>, [888-455-1864](tel:888-455-1864) passcode: 3611044

User Group Meeting

- **Tuesday, August 16, 2016, 9:00am - 12:00pm**
- Location: GSA Central Office 1800 F St., NW room 4143
- [888-455-1864](tel:888-455-1864) passcode:5887

Registrar Classroom Training

- **August 17 - 18; September 21 - 22**
- Location: HPE, Chantilly
- Contact [Jim Schoening](#) for information

Delay in Release date for 9.10 and 10

As a result of the Entrust ATO expiration Release 9.10 and Release 10, previously

scheduled for July 23, is being held for final technical review and determination. Agency Leads will be notified as soon as release details are finalized. Agencies should continue with plans to upgrade their Light systems to v4.0.3 (as discussed in previous Blue Tops) as soon as possible as the upgrade is still required once Release 9.10 goes in to production. Please see the release notes for Light Installers v4.0.3 and Release 10 on the Agency Lead Portal.

Customer Access Control List Update

Entrust has informed us that they will be pushing an update to the Customer Access Control list on July 30, 2016, for the following service: <http://sspweb.managed.entrust.com>.

If you are using an FQDN to reach the above URL, this change will be transparent to you. **If you filter by IP address at the firewall**, please go to the following website to receive the new Customer Access Control

whitelist: <https://trustedcare.entrustdatacard.com/TrustedCare/articles/Technote/Akamai-CAC>.

This change will take place on Saturday, July 30th 2016. Remember that if you are whitelisting by IP address at the firewall, you must enter the new IP address list to prevent possible disruption to your service. If you are not whitelisting by IP address, you will not experience any disruption to your service.

Please make sure to notify your network security team so they can make any necessary changes. If at any time you require assistance, please contact Entrust Datacard Managed Services support by phone at [1-877-237-8754](tel:1-877-237-8754) ([1-613-270-3715](tel:1-613-270-3715) outside of North America) 24x7x365 or by email at support@entrust.com. If you have any additional questions, please do not hesitate to contact the GSA Managed Service Office at GSAMSO@gsa.gov.

Entrust ATO Status

The GSA Office of Governmentwide Policy has issued an extension letter dated July 26, 2016 for Entrust ATO through October 31, 2016. The MSO is continuing to work with the Office of Governmentwide Policy to assist with the process of renewing the authority to operate. At this time there is no change to the services being offered. Should any status change the MSO will notify Agency Leads.

Reminder to Review the Registrar Daily Checklist

The Registrar Daily Checklist was updated in December of 2015. Registrars are reminded to follow the Registrar Daily Check list **every day**. The checklist applies to both LCS kits and Fixed stations.

The Registrar Daily Checklist is available on TRACKS under [Job Aids](#). The Checklist document explains what is necessary to complete each step, providing the detail needed to actually complete the steps. Please be sure to go to TRACKS and download the updated version. It is a good idea to print out the checklist and have it handy so you can start each day by going through the list.

The steps are:

1. Workstation Logon and Reboot
2. Look for Advisories on TRACKS Web site
3. Fingerprint Scanner
4. Flatbed Scanner
5. Camera
6. GSA Online Scheduling System Login
7. USAccess (Assured Identity) Login and System Test - Please do NOT to save the TEST records used use to test the enrollment portion.
8. End of Day Checklist

Remember to subscribe to the Blue Top Newsletter



We have modernized the way we deliver the Blue Top with the help of GovDelivery which is an email subscription service that makes it easier to manage and track distribution lists. GovDelivery allows recipients to subscribe and unsubscribe themselves with just a few clicks of their mouse. Everyone who is already on the Blue Top distribution list will not have to do anything to receive the newsletter as you have already been added to the distribution list.

However, anyone who has been forwarded this email and wants to add themselves to the distribution list can click the green envelope link (pictured) in the "Stay Connected" section of the footer at the end of this newsletter or follow [this link](#) to subscribe themselves. Follow the prompts to enter your email address and an optional password. You will then be able to pick the newsletters you want to receive. Click "USAccess Blue Top" in the "Integrated Technology Services" section within the "IT Services" dropdown.

Service Enhancements

Changes/updates since last Blue Top

- Updated USDA Zone 4 Return Address
- Modified Zone 17 for Department of Energy (DOE)

Planned changes

- Routine maintenance is scheduled for Saturday, August 6. Please plan for the USAccess service and role holder portals to be unavailable for most of the day.

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

Security Tip

Caution for Social Engineering Attacks

Be wary of phone calls or emails from unknown people requesting information on an applicant or USAccess credentialing. Because of your USAccess Role you may be a target of Social Engineering. This is where someone attempts to gain information from you through manipulation. If you are unsure of the validity of the caller or emails you asking for sensitive information, it's okay to say NO. If possible call the agency directly to verify credentials before giving out any information.

If you are the target of a Social Engineering attack make sure you report it to your security office.

To subscribe to this newsletter click the green envelope in the "Stay Connected" section of the footer below.

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

STAY CONNECTED:

