How to Use Your LincPass Credential

(Quick Reference Guide for GIPSA Users)

Your LincPass is your USDA personal identity verification (PIV) card. This guide explains how to use your card and PIN to access and protect USDA network and computer resources.

What You'll Need to Get Started

- LincPass (USDA's smartcard)
- PIN
- Card reader and drivers installed on your computer
- Card reader software installed on your computer
- HSPD-12 enabled account on your agency's network

NOTE: Two-Factor Authentication has been implemented for Windows users; other operating systems will be addressed in a later phase.

Everyday Use

Computer Connected to the Network

Logging In

1. Start your computer.
2. When the Windows login message box appears,
   - Insert your card in your computer's card reader.

3. Click OK at the "government system" warning. In the login dialog box, enter your 6- to 8-digit PIN.

4. After you log in, an ActivClient icon will appear in the Windows system tray (lower right). This will show you whether or not the card is being read.

Card In: Card Out:

Terms & Definitions

LincPass: As part of ensuring national security, Homeland Security Presidential Directive 12 (HSPD-12) mandates that Federal agencies properly identify and credential employees and contractors before allowing any access to federal buildings for information systems. One of the requirements of HSPD-12 was the use of "smartcards"— that meet National Institute of Standards and Technology (NIST) guidelines for physical and logical access to federal buildings and information systems.

PIN: Personal Identification Number, 6 to 8 digits, which you chose and entered when you activated your LincPass. Your PIN allows you to access and use your card; your card allows you access to the network.

Two-Factor Authentication: Within USDA two-factor authentication is based on something you have and something you know. The use of two-factor authentication by using the LincPass for logical access greatly increases the assurance that you are authorized to access USDA systems.

LincPass Enrollment Station: A fixed enrollment station is a permanent location with a GSA-provided computer, equipment, and operator who handles enrollment and activation of USDA LincPass cards (also handles PIN resets). There are a few mobile enrollment stations that are temporarily assigned to a series of locations for the purpose of enrolling staff, but cannot handle PIN resets. There are also several *Light Activation Stations* deployed nationwide that can handle PIN resets and card activations. NOTE: USDA employees can only enroll and activate credentials at SHARED sites. Do NOT make appointments at DEDICATED sites as those are reserved for employees of those agencies only.

To locate the nearest activation/enrollment station visit the USAccess website at: **http://www.fedidcard.gov/**

HSPD-12 Security Officer: The person designated by your agency with responsibility for responding to LincPass security-related events, such as lost or stolen cards, card suspension & activation, etc. The email for LincPass issues on lost/stolen/damaged cards is LincPass.Securitys@APHIS.usda.gov

Network Credentials: The user ID and password you use to access your agency's domain without a LincPass.

Certificates: Encrypted sets of electronic credentials loaded on your LincPass.

How to Use Your LincPass Credential

(Quick Reference Guide for GIPSA Users)

Locking and Unlocking Your Computer

By default, removing the LincPass from the reader ***should*** automatically lock the workstation. If it does not you need to contact ATAC.

IMPORTANT: Don't forget to take your card with you when you leave your workstation.

Logging Off Your Computer

From the Windows Start menu, click "Shut Down" (or "Log Off [username]"), then follow the standard procedure for Windows.

TIP: Don't remove the LincPass while shutting down the computer, because the automatic "lock workstation" or "log off user" feature will override the shutdown procedure. Wait until the computer sequence is finished before removing your card.

Computer NOT Connected to the Network

1. Start your computer.
2. When the Windows login message box appears, put your card in the card reader.
3. In the login dialog box, enter your 6- to 8-digit PIN.
4. From here, you can access anything on your local computer. You can also connect to the Internet as you usually do, such as via a hotel network or wireless access.

LincPass vs. Network Credentials

Both the LincPass and your network credentials (user ID and password) can be used to access your network – both are active. However, to increase the security on the network and for greater protection of your digital identity, the LincPass card is required for use when connecting to the GIPSA network and for all eAuthentication websites such as WebTA, NFC and AgLearn.

Telework

To access the GIPSA network you must first connect to AnyConnect, the VPN solution used in GIPSA. Use the LincPass Smartcard as the profile selected.

Contact your local IT staff for guidance if your computer does not have AnyConnect loaded on your PC.

Care of Your LincPass

Your LincPass is intended to last 5 years. **(Digital Certificates must be recertified/updated every 3 years.)** It is expensive and time-consuming to replace if lost or damaged. You should guard your card the way you do your driver's license or house key. Protect it from excessive heat or cold, scratches, bending, and magnets. Use only approved badge holders or those provided by your agency because some types of plastic badge holders will degrade the ink on the face of the card. If you notice your card reader is damaging your card, get your card reader replaced — it's much less expensive than the card. A LincPass is considered government property and must be shown to security personnel upon request and surrendered upon employee or contractor termination.

Get in the habit now of taking your LincPass with you whenever you leave your desk, your LincPass is your official ID for building or office access.

Forgot LincPass

If you don't have your LincPass (but it's not lost or out of your control), you can log into your network using your network e-authentication credentials until you have your LincPass again. Remember to follow the procedures described above in the *LincPass vs. Network Credentials* section.

Forgot PIN /Locked PIN

IMPORTANT: If you make 6 unsuccessful attempts in a row to type your PIN, it is automatically locked and will need to be reset. If you forget your PIN or have locked your access you must visit a USAccess Center to have the PIN reset. Most locations require an appointment prior to the visit. You can locate the center that is closest to you at the following web address:
http://www.fedidcard.gov/

Change PIN

If you want to change your PIN, use the ActivClient Agent. You can access the PIN Change Tool from the Start|Programs| ActivIdentity| ActivClient| menu, or from the ActivClient user console, which is available from the same menu or by double-clicking on the ActivClient icon in your system tray.

How to Use Your LincPass Credential

(Quick Reference Guide for GIPSA Users)

Lost/Stolen/Damaged LincPass

If your LincPass is damaged, lost, or stolen; send an email message to LincPass.Security@APHIS.usda.gov providing your full name, phone number, program information, current duty station, and detailed explanation of the event. Security will alert you to the next steps, including potential re-enrollment for a new LincPass, if lost or stolen. Use your network credentials in the interim until your new card arrives and is activated. If your building's physical access control system uses the LincPass for access, you will also need to request a temporary or visitor's card to get into your work location.

If your LincPass card is damaged, e.g., melted, bent, etc., contact your HSPD-12 Security Officer, who will revoke the card, and ask your sponsor to issue a reprint request in the system. If your building's physical access control system uses a LincPass for access, you will also need to request a temporary or visitor's card to get into your work location

If you find someone else's LincPass, give it to your HSPD-12 Security Officer, who will either get it to the right person or send it to the "Return to" address on the back of the card.

Change to Visible Information on LincPass

If information about you that appears on the face of your LincPass changes (e.g., name change), your office should submit a name change request through HRD's personnel action request process. Remember to also send the information to LincPass.Security@APHIS.usda.gov. You will be then be notified when to go through the enrollment process again. Use your network credentials in the interim until your new LincPass arrives and is activated. If your building's physical access control system uses a LincPass for access, you will also need to request a temporary or visitor's card to get into your work location.

Employment Status Change and Your LincPass

If your employment status changes from active to suspended, the HSPD-12 system will receive the status change and automatically suspend your LincPass. When employment status in the HR system changes from "suspend" to "terminate," HSPD-12 system automatically revokes/terminates the LincPass. Give the LincPass to the designated HSPD-12 Security Officer for proper disposal.

If a former employee returns to employment status in the HR system (terminate to active), the newly activated employee will need to be sponsored for a new LincPass and go through the enrollment and activation process again.

Certificate Recertification/Update vs. LincPass Credential Renewal

There is a BIG Difference!

➢ ➢ ➢ **3 YEARS**

Certificate Recertification/Update

Your LincPass has certificates loaded on the chip (the part that makes the card a "smart" card), including an authentication certificate and a digital signature certificate.

The digital certificates on your LincPass card expire ***3 years after the certificate issuance date***. Employees receive an email from the HSPD-12 USAccess system of the need to recertify/update the digital certificates. The email will provide instructions on how to recertify these certificates. **If you do NOT renew the digital certificates, the LincPass credential automatically terminates and you will be required to re-enroll to receive a new functional card.**

➢ ➢ ➢ ➢ ➢ **5 YEARS**

LincPass Credential Renewal

Your LincPass will expire ***5 years*** after the issue date (*the expiration month and year are also shown on the face of your card*). You will receive a system generated email notification from **HSPD12Admin@usaccess.gsa.gov** providing instructions on making arrangements to pick up and activate the new credential. You'll keep your old LincPass until you pick up the new card. The individual activating your new credential will dispose of the old card.

How to Use Your LincPass Credential

(Quick Reference Guide for GIPSA Users)

Where to Go for Help

To obtain help related to the *daily use* of your LincPass, **START FIRST** by calling: your local assigned IT support team.

COMMON RECURRING ISSUES	WHO TO CONTACT	ACTION REQUIRED by CONTACT
LOST/STOLEN Card OTHER Card Issues - Card Damaged - Photo Fading - Laminate Separating - Wrong Photo - Someone else's name - Incorrect Biometrics o Hair/Eye color o Height	Send email to: **LincPass.Security@APHIS.usda.gov** Include: • Full Name *(also include in subject line of email for easier tracking)* • Program (examples below) o GIPSA, OA, Mngmt & Budget o GRAIN, FMD • Supervisor's Name • Duty Station • Brief Information regarding card problem/issue	CARD REPRINT
Name Change	1. HR Processing (SF-52 Action Required) 2. email to **LincPass.Security@APHIS.usda.gov**	CARD REISSUANCE (Employee Needs to Re-enroll)
Card Quit Working (1) in Door Card Reader (if used)	Your local Facilties/Security	Lenel System Account Needs Review for Correct Permissions
(2) in Computer	Local IT support team	Logical Access Needs ITD Review
CARD ISSUANCE STATUS	Send email to: **LincPass.Security@APHIS.usda.gov**	
CARD RE-ROUTING SCHEDULING APPOINTMENTS EXPIRED LINCPASS CREDENTIAL EXPIRED DIGITAL CERTIFICATES	HSPD12 HELP DESK at: USDAHSPD12HELP@dm.usda.gov (or) 1-888-212-9309	CARD REISSUANCE (Employee Needs to Re-enroll)
CARD DESTRUCTION	Send email to: **LincPass.Security@APHIS.usda.gov**	

(1) When a LincPass credential stops working, it is NOT assumed to be defective until the e-PACs, or electronic Physical Access Card Reader Systems, can be checked for operability and permissions.

(2) There may be information technology system issues or updated versions of your computer's ActivClient software for the LincPass certificates to work properly.