USDA Office of the Chief Information Officer — Identity and Access Management

Two-Factor Authentication

How to Use Your LincPass

Your LincPass is your new USDA personal identity verification 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 Start

- 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

NOTES: (1) Two-Factor Authentication is being implemented for Windows users; other operating systems will be addressed in a later phase. **(2)** You may have two cards for awhile, your LincPass plus a separate card for building access.

Everyday Use

Computer Connected to the Network

Logging In

1. Start your computer.
2. When the Windows login message box appears,

put 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.

An ActivClient icon in the Windows system tray (lower right) will tell 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 screen their employees and contractors and issue credentials—"smartcards"—that meet National Institute of Standards and Technology (NIST) guidelines by October 2008. In USDA, the smartcard is called a LincPass. NIST's term is "personal identity verification" or PIV card.

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.

Card reader: A device built in, added, or connected to your computer that reads smartcards.

Card reader software: The client application installed on your local computer that integrates the card with your agency's network.

HSPD-12 enabled account: A user account on an agency network that is integrated with HSPD-12 and enterprise services. Your agency will notify you when network accounts have been enabled for LincPass use.

UPN: User Principal Name. Used by agency networks as the user ID for HSPD-12 enabled accounts.

Two-factor authentication: Authentication can be based on what you know, what you have, or what you are. "Two-factor authentication" means using a two of these authentication methods (LincPass + PIN) to increase the assurance that you are authorized to access USDA systems.

Laptop: Self-contained portable computer used to access USDA resources. The Two-Factor Authentication rollout begins with laptops.

LincPass enrollment & activation station: GSA-owned computer, equipment, and operator who provides enrollment and activation of USDA LincPass cards (also handles PIN resets).

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.

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

Locking & Unlocking Your Computer

By default, removing the LincPass from the reader will automatically lock the workstation. However, your agency's network policies dictate the process for locking and unlocking your computer. Your agency will provide you with more detailed information. **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 locking or 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

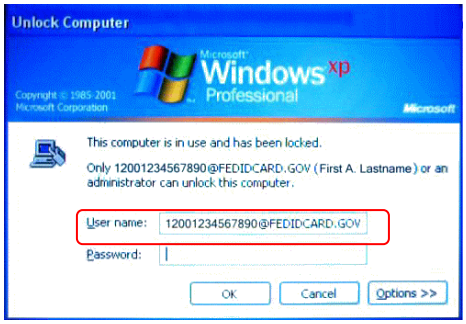
1. Start your computer.
2. When the Windows login message box appears, put your card in the card reader.
3. In the login dialog box, enter your 6- to 8-digit PIN.

4. From here, you can access anything on your local computer. You can also connect to the Internet as usual, such as via a hotel network or wireless access.

LincPass vs. Network Credentials

For the transition period during the rollout period in which your agency is implementing LincPass use, either your LincPass+PIN or your network credentials (user ID and password) can be used to access your network – both are active. Once the rollout is complete, you'll be required to use your LincPass. In the interim, here are some things to keep in mind:

1. If you log in with your network credentials, you may later put your LincPass in the reader, but removing it won't have any effect — you'll have to use lock or logoff your computer using Windows menus (e.g., *Ctl+Alt+Del*).
2. If you log in with your LincPass+PIN, then lock the computer, then press *Ctl+Alt+Del* to restore the system instead of using your card, your user ID will look like an email address that starts with 1200 followed by 10 numbers (see below). This is your UPN, which replaced your user name for an HSPD-12 enabled account.



DO NOT ERASE THE CONTENTS OF THE USER NAME FIELD! Instead, go to the password field and **enter your network credentials password** (**NOT** your PIN!).

3. If you log in with your network credentials and use *Ctl+Alt+Del* to lock your computer, you may use your LincPass to unlock it by inserting your card and entering your PIN at the prompt.

Care and Feeding of Your LincPass

Your LincPass is intended to last 5 years, and 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 the key to your house. Protect it from excessive heat or cold, scratches, bending, and magnets. Also, some types of plastic badgeholders will degrade the ink on the face of the card, so only use approved badgeholders or those provided by your agency. 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.

NOTE: Get in the habit now of taking your LincPass with you whenever you leave your desk, since your LincPass may soon be your official ID for building or office access. Until your location's access control is integrated with HSPD-12, you may need to carry both your LincPass and your building access card.

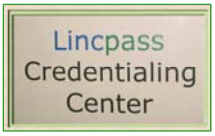
How to Use Your LincPass

LincPass Issues

Forgot LincPass

If you don't have your LincPass (but it's not lost or out of your control), during the transition period, you can log into your network using your network credentials until you have your LincPass again. Remember to follow the procedures described above in the *LincPass vs. Network Credentials* section. Once the LincPass is required and you forget to bring it, follow your agency's policy on gaining temporary access.

Forgot PIN / Blocked PIN

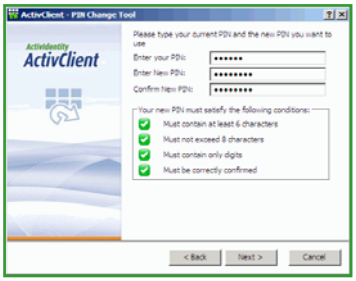


If you make 6 unsuccessful attempts in a row to type your PIN, it is automatically blocked and will need to be reset. If you forget your PIN, you must first block it by making 6 unsuccessful attempts. To get your PIN unblocked, take your LincPass to the nearest HSPD-12 activation station and ask to have your PIN unblocked.

Depending on the location, you may need to make an appointment first. The activator will ask you to verify your fingerprint (to ensure the card belongs to you), and to enter a new PIN.

Change PIN

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



Your PIN must meet complexity requirements, including no doubled numbers or obvious sequences.

Lost/Stolen LincPass

Report your lost/stolen LincPass to your designated Security Officer, who will suspend or revoke your card depending on the circumstance. If you find your card within **5** business days, take it to your designated Security Officer to reactivate it. After **5** business days, the Security Officer will revoke the card and you will have to re-enroll for a new LincPass. Use your network credentials in the interim until your new card arrives and is activated. If your building's physical access control system uses a LincPass for access, you may 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 designated 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., you change your name, first notify your sponsor, who will request a new card, then give your current (now revoked) card to your Security Officer for proper disposal. 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 may also need to request a temporary or visitor's card to get into your work location.

Damaged LincPass

If your LincPass is damaged, e.g, melted, bent, etc., turn it in to your designated Security Officer, who will revoke the card, and mark in the HSPD-12 system that you need a new card. You'll have to go through the enrollment process again, and use your network credentials in the interim until your new card arrives and is activated. If your building's physical access control system uses a LincPass for access, you may 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.

How to Use Your LincPass

When employment status in the HR system changes from "suspend" to "terminate," the HSPD-12 system automatically revokes the LincPass, which should be given to the designated 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.

LincPass Renewal

Your LincPass will expire 5 years after the issue date (the expiration month and year are shown on the face of your card). You and your sponsor will be notified via email from the HSPD-12 USAccess system of the need to renew your LincPass. The email will give you instructions on signing up for an enrollment appointment. You'll keep you old LincPass until your new one arrives and is activated, then turn in your old card to your designated Security Officer for disposal.

Certificate Renewal and Reissuance

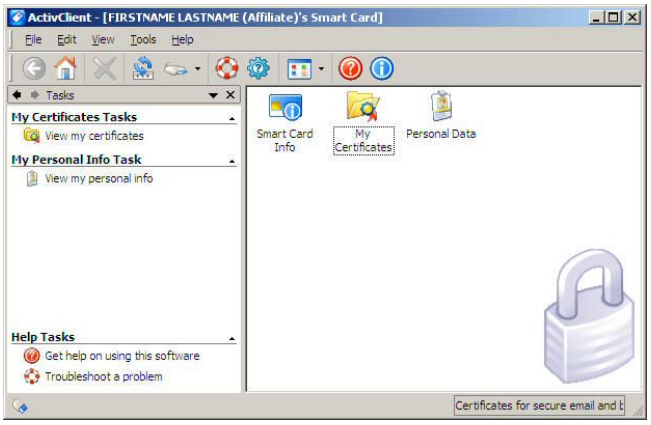
Your LincPass has certificates loaded on the chip (the part that makes the card a "smart" card), including an authentication certificate and a digital signature certificate. LincPass certificates expire 3 years after the certificate issuance date. You'll receive an email from the HSPD-12 USAccess system of the need to renew your LincPass certificates. The email will provide instructions on how to renew certificates.

ActivIdentity Client Card Reader Software

The ActivIdentity Client card management software enables your operating system to pass your card's certificates the network.

Access the user console by double-clicking the icon in the Windows system tray, or from the Windows Start menu, choose **Programs | ActivIdentity | ActivClient | User Console.**

From the console, you can see information about your card, the certificates on your card, change your PIN (as described earlier), and run the Trouble-shooting wizard or the Diagnostics tool.



When you double-click the My Certificates icon, you can see your card has four certificates: PIV Authentication Key (for accessing the network), Digital Signature Key (future use, for sending digitally signed email), Key Management Key (future use, for encryption), and Card Authentication Key (for allowing the system to access the card).

> **NOTE:** Your **PIV Authentication Key** stores the UPN associated with your card. Double-click the certificate's icon, then go to the Advanced tab. Toward the bottom of the list, click on the "Subject Alternative Name" item. The window below displays a "Principal Name=" followed by your UPN, e.g., 12001234567890@FEDIDCARD.GOV

Where to Go for Help

Follow your agency's instructions and policies for getting help with Two-Factor Authentication issues.

For general USDA Two-Factor Authentication information, visit http://hspd12.usda.gov/twofactor.htm. For information on the USAccess system, GSA's HSPD-12 service for all federal agencies, visit http://www.fedidcard.gov.

You may also contact the ARS LincPass Sponsor at:

Tamara Staley
Email: Tamara.Staley@ars.usda.gov
Phone: 301-504-1332