Air Force Research Laboratory

Lightweight Portable Security (LPS) Public Edition (LPS-Public) User's Guide

Version 1.6 – 17 July 2015

DISTRIBUTION A — Approved for public release; distribution is unlimited.

AFRL/RYWA
2241 Avionics Circle, Bldg. 620
Wright-Patterson AFB, Ohio 45433-7320

88 ABW-10-0024, approved 5 January 2010

TABLE OF CONTENTS

1 Quick Start 1

2 Introduction 2

2.1 Using LPS to Improve Security 2

3 Getting Started 4

3.1 System Requirements 4

3.2 Hardware Setup 4

3.3 Starting LPS 6

3.4 Boot Messages 8

4 Using LPS 10

4.1 The LPS Desktop 10

4.2 Connecting to the Network 14

4.3 Browsing the Internet 22

4.4 Using a Smart Card 23

4.5 Using Email 24

4.6 Using Instant Messaging 31

4.7 Saving Your Work 31

4.8 Working with Compressed Files 34

4.9 Printing 34

4.10 Using DCS for Online Collaboration 37

4.11 Using Adobe Reader to Sign Forms 38

4.12 Using SharePoint 39

4.13 Encrypting Data 41

4.14 Adjusting LPS Security Settings 42

4.15 Create your own bootable LPS USB Flash Stick 42

5 Addressing Common User Problems 44

5.1 Hangs During Booting 44

5.2 Can't Connect via WiFi 44

5.3 Can't Access PKI web sites 45

5.4 Need to Sign or Encrypt Email Messages 45

5.5 Need to work with Lotus Forms (XFDL files) 46

5.6 Not Working with Multiple Monitors or Docking Station 46

5.7 Problems Using Dell Keyboard with Integrated CAC Reader 46

5.8 Can't use some 4G Wireless Cards 46

5.9 Sound Garbled in Citrix 47

6 Troubleshooting 48

6.1 Unable to Boot from CD 48

6.2 Unable to Boot from a Flash Memory Stick 49

6.3 Hangs During Booting 49
6.4 Unable to Access the Network 50
6.5 Unable to Access Local Drives 51
6.6 Unable to use a Smart Card 51
6.7 Defense Travel System (DTS) Doesn't Work 53
6.8 No Sound 53
6.9 No Printing 54
7 Support 55
7.1 Warranty 55
7.2 License 55
7.3 Copyrights 55
7.4 Contacts 56

LIST OF FIGURES

Figure 1 — LPS Starting Screen 6
Figure 2 — LPS Boot Menu 6
Figure 3 — LPS Loading 7
Figure 4 — LPS UEFI Boot Menu 7
Figure 5 — Startup Screen 8
Figure 6 — LPS User Agreement Dialog Box 8
Figure 7 — LPS User Agreement 9
Figure 8 — Smartcard Reader Not Detected 9
Figure 9 — LPS-Public Desktop 10
Figure 10 — LPS-Public Deluxe Desktop 14
Figure 11 — Connection in Progress Icons 14
Figure 12 — Successful Connection 14
Figure 13 — Active Connection Indicators 15
Figure 14 — Active Connection Detailed Information 15
Figure 15 — Disconnected Status Indicators 15
Figure 16 — Edit Connections in Network Manager 15
Figure 17 — Adding a New Wired Connection 16
Figure 18 — Selecting a Manual IP Configuration 16
Figure 19 — Setting Static IP Address 16
Figure 20 — Successful Static IP Address Created 17
Figure 21 — Initiating a Static IP Connection 17
Figure 22 — Available Wireless Networks 18
Figure 23 — Wireless Authentication Dialog 18
Figure 24 — Initiate Cellular Broadband Connection 19
Figure 25 — Setup Cellular Broadband Connection 19
Figure 26 — Select Cellular Broadband Country 20
Figure 27 — Select Cellular Broadband Provider 20
Figure 28 — Complete Cellular Broadband Connection 21
Figure 29 — Successful iPhone Tethering 21
Figure 30 — iPhone Display with Tethering Enabled 22
Figure 31 — Certificate Selection 23

Figure 32 — CAC PIN Request from Firefox 24
Figure 33 — Email Setup Dialog 26
Figure 34 — OWA URL Input Dialog 26
Figure 35 — DavMail Gateway Launch Message 26
Figure 36 — DavMail PIN Entry and Certificate Selection 27
Figure 37 — Thunderbird Client with Message Headers Downloading 27
Figure 38 — Instant Messaging Add Account Dialog 31
Figure 39 — USB Device Mounted on Desktop 32
Figure 40 — Safely Remove USB Storage 33
Figure 41 — USB Device Opened in File Manager 33
Figure 42 — CD Mounted on Desktop 33
Figure 43 — Browsing a CD 34
Figure 44 — Ejecting a CD 34
Figure 45 — Printer Administration Screen 35
Figure 46 — Local Printer Detected 35
Figure 47 — Choosing a Network Printer 36
Figure 48 — Creating a Network Print Queue 36
Figure 49 — Local and Network Print Queues Defined 37
Figure 50 — Print Queue Status 37
Figure 51 — BIOS Setup Screen 49
Figure 52 — DBsign Client Configuration Screen 53

1 Quick Start

For experienced users, here is the short version of how to get started using LPS:

1. Make sure your computer is configured to boot from a CD or USB stick.
2. If using a wired Ethernet network, connect your computer to a network port.
3. Connect any external devices you will be using (hard drive, smart card reader).
4. Insert your smart card, if you want to visit CAC- or PIV-enabled websites.
5. Insert the LPS CD into the CD-ROM drive, or the USB stick into an open USB port.
6. Boot the computer, verifying that LPS is loading.
7. If using a wireless Ethernet or cellular broadband network, use the Network Manager utility to connect to it.
8. Launch Firefox and check that network connectivity exists.
9. Use the browser or run other loaded applications.

Note that LPS is designed to be run on home computers connected to the Internet. It is not designed to run while connected directly to government networks, and it may not boot properly on a government-issued standard desktop computer unless the system allows booting from a CD.

2 Introduction

Lightweight Portable Security (LPS), Public Edition (LPS-Public) is a security-focused Linux boot disc with a small memory footprint. It creates a pristine, trusted end-node within the volatile memory of an unmanaged computer system. LPS boots a small operating system from a CD-ROM without mounting the internal hard drive, thus bypassing any resident malware. Since a local hard drive isn't mounted, no persistent user session data is saved. Each time LPS boots, a trusted, known, read-only configuration is loaded.

LPS-Public can be used for many different situations where secure access is needed using untrusted systems:

- Minimizing the risk to corporate networks from untrusted computers (e.g., home computers, hotel business center PCs).
- Allowing secure remote access while controlling the outflow of data.
- Browsing the Internet without leaving traces of financial transactions, browser history, personal data, corporate information, or other private data on the host computer.
- Keeping personal data segregated from corporate data.
- Bypassing software keyloggers, persistent malware, or other rogue software.
- Allowing for fast, easy, low-cost continuity of operations (COOP) or business continuity.
- Quickly creating a secure end node using home computers of government personnel.
- Allowing a single computer to be used in multiple roles while traveling, obviating the need to bring along multiple systems.
- Providing a "Plan B" for systems that are broken, locked-out, or are otherwise rendered unusable while traveling.

The standard LPS-Public distribution includes the Linux operating system, a smart card-enabled Firefox web browser with Java and Flash support, Encryption Wizard, PDF viewer, a file browser, Remote Desktop Software (Citrix, Microsoft, or VMware, SSH client, and the ability to use USB flash drives and portable hard drives. However, LPS can be customized for particular government or corporate missions and security requirements—including adding VPN clients and custom applications. This custom version is known as Bootable Media, and is available for free to the US Department of Defense (DoD) and for a nominal fee to other US government agencies.

This User's Guide describes the features of the standard LPS-Public distribution and some of the most popular options. Please understand that not all features may be present in all versions of LPS. If you need features not present in your version of LPS, contact your computer support staff and request a customized distribution.

2.1 Using LPS to Improve Security

LPS differs from traditional operating systems because it is not continually patched. While this may seem like a disadvantage, it is a result of its unique design. LPS is inherently more secure than most operating systems since it is architected to run from read-only media and has no

persistent storage. Any malware that might infect a computer can only run within that session. A reboot can clear any memory-resident infection.

A user can improve security by rebooting between sessions, or when about to conduct a sensitive online transaction. For example, boot LPS immediately before performing any online banking activities. LPS should also be rebooted immediately after visiting any risky web sites, or when the user has reason to suspect malware might have been loaded. In any event, rebooting when idle is an effective strategy to ensure a clean computing session.

When using LPS on a USB flash drive, never use the LPS boot device for data storage – use a separate writable drive. If your LPS boot stick is used as writeable storage, persistent malware could be loaded. LPS boots much faster (2-5x) from a USB flash drive than from a CD. If you intend to reboot frequently, running LPS from a boot stick can improve your experience. LPS boots about twice as fast from a DVD as from a CD due to higher disc compression rates.

LPS is updated on a regular basis (quarterly maintenance releases, typically). Update to the latest versions to have the latest protection and functionality. When you launch Firefox, the default home page will be updated whenever you have an outdated version. Look for the red notice when a new version is available. You can also sign up on the LPS web site to be notified when new releases of LPS are shipped.

3 Getting Started

3.1 System Requirements

LPS has fairly limited requirements since Linux is not a resource-intensive operating system, and extraneous functionality has not been loaded. Basic LPS functionality requires:

- A computer system with an x86 processor supporting Physical Address Extension (PAE). PAE was first introduced in the Pentium Pro chip in 1995, and is present in all later chips except early versions of the Pentium M laptop chips. PAE is present in AMD Athlon and later processors. LPS is supported on standard Wintel-type PCs and Intel-based Macs.
- A minimum of 1 GB RAM (1.5 GB for Deluxe). More RAM will give more working space and allow more applications to be run simultaneously.
- Ability to boot from CD-ROM or USB memory stick.
- Wired, wireless or cellular broadband Ethernet connection (DHCP highly recommended).
- CCID-compliant USB smart card reader (if accessing PKI-enabled websites). Generally works best when connected to a USB2 port; some USB3 ports apparently do not work well.
- USB-connected or local network printer (if printing is desired).

LPS should work with all CCID-compliant, USB-connected smart card readers. Check data sheets or product documentation for the readers to determine if they support these standards. LPS has been extensively tested with the SCM SCR331 reader, one of the most common models within the DoD. Some readers require a firmware update for CCID compliance; a firmware updater is included within LPS for several readers, including the SCR331. LPS is not fully supported using internal smart card readers; some might work, but others don't. Smart card readers integrated into keyboards generally work. Some features may not work well if multiple smart card readers are connected.

3.2 Hardware Setup

In order to run LPS, you must be able to boot from a CD or from a USB flash drive. The process is different on Macs and PCs due to architectural differences in the platforms.

On a Mac, you can boot from a CD simply by holding down the "c" key during the boot process or by holding down the *option* key during the boot process and then selecting the EFI Boot option (for USB flash drives) or the CD as boot device (the CD may show up as a Windows disc). Bluetooth keyboards and mice on Macs may need to be woken up before they can be recognized. Shutting down and restarting the computer often works better than restarting from within the Mac OS.

If these approaches do not work, boot your Mac normally then run the System Preferences utility in the Applications folder. Select Startup Disk. Choose the CD device, which may be labeled "Foreign OS on CDROM", then restart the Mac. Note that this procedure requires administrator credentials. If booted in this manner, the CD must be ejected in order to boot back into Mac OS X. Hold down the mouse button during the reboot process to eject the CD.

On a PC, the process can be quite a bit more complicated. First, confirm that your BIOS boot priority lists the CD or USB drive *before* the internal hard drive. Often the easiest way to confirm this is to simply attempt to boot from the CD. If the LPS loading screen appears (Figure 1), you are booting from the CD. If your home operating system loading screen appears, you are booting from the internal hard drive. Some PCs provide a boot menu where you can make a one-time selection of the boot device; if you have a computer like this, you should select whichever device contain the LPS boot media (CD or USB).

If your PC is not configured to boot from CD by default, reboot the computer and enter the hardware setup screen. This usually involves pressing certain key(s) during a specific part of the boot process. The specific keys vary by hardware manufacturer and model, and are often a function key (e.g., F1, F2, F9, F10, or F12). The keys should be identified in the user's guide for the computer, and are sometimes displayed on the screen during the boot process. Depending on the speed of your computer and certain configuration settings, the interval where the setup key is recognized can be quite narrow. If the operating system on the computer's internal hard drive starts to load (e.g., if you see a Windows startup screen), you missed the interval where the key can be pressed—restart and try again.

The process may be further complicated if your system was designed to be used with Microsoft Windows 8 or newer. These systems use the Unified Extensible Firmware Interface (UEFI) to boot the system. UEFI replaces the Basic Input/Output System (BIOS) firmware found in almost all previous PCs. LPS 1.6.0 introduced support for loading from USB on systems that use UEFI, such as Apple Mac computers with Intel chipsets and these newer Microsoft Windows 8 compatible PCs. While not an option on Mac based systems, PCs do often provide an option in their firmware to use BIOS/Legacy or UEFI boot from both the setup and boot menus.

LPS is currently incompatible with the Secure Boot feature enabled on many systems that come preinstalled with Windows 8 and newer. You may disable this feature permanently or temporarily from within the system firmware setup (formerly BIOS) without impacting your Windows installation. The Secure Boot feature prevents loading of software that is not recognized by Microsoft. The LPS team is working on registering as a recognized system for a future release.

If you intend to use wired Ethernet, connect your computer's Ethernet network port to a live network connection. LPS works best when the network uses the Dynamic Host Configuration Protocol (DHCP) service for assigning a unique network address to your computer. If you intend to use wireless Ethernet (WiFi) or cellular broadband modems, you will configure this after LPS boots.

If you intend to use a CAC or PIV, connect the external smart card reader to an available USB port on your computer. Internal smart card readers are not fully supported; some may work but several don't. Insert your CAC or PIV into the smart card reader.

3.3 Starting LPS

Place the LPS CD in your computer's CD drive or connect an LPS stick to an open USB port. Boot the computer. If you're booting from BIOS/Legacy mode, you should see the LPS startup screen, as shown in Figure 1:

Figure 1 — LPS Starting Screen

If any key as pressed at this point, you will be presented with a menu allowing you to change boot options as show in Figure 2. The menu provides access to workarounds for hardware issues, such as the **Basic Video Mode** option for working around issues with unsupported graphics devices.

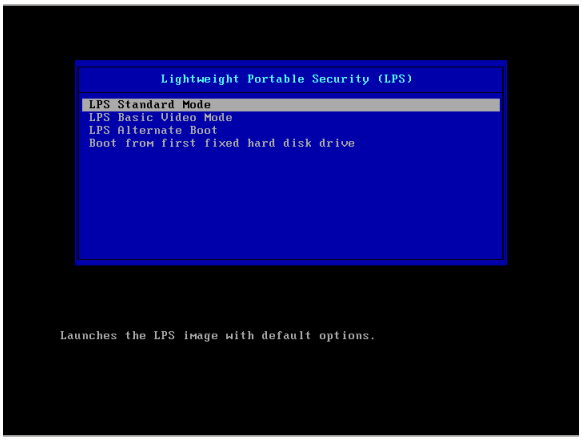

Figure 2 — LPS Boot Menu

Regardless of whether the menu is used, LPS will begin loading from media into memory as shown in Figure 3. LPS can take a few minutes to load since CD drives are typically slower than hard drives. Faster processors, more memory, and faster CD drives can speed up this process; burning LPS to a DVD rather than a CD can double the boot speed. If you are booting from a fast USB memory stick, you can be ready to go in less than a minute.

Figure 3 — LPS Loading

If your system is booting from UEFI mode, you will instead be presented with the menu in Figure 4. Unfortunately, the UEFI loader does not present the user with a progress indicator when loading the operating system from media, and instead displays a blank screen as the loader screen.

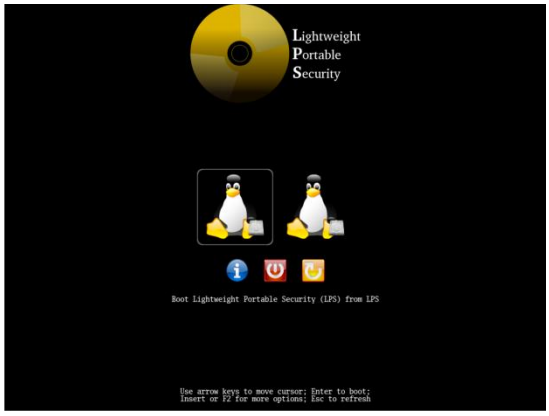

Figure 4 — LPS UEFI Boot Menu

Once LPS is read from media using either the BIOS/Legacy or UEFI boot process, you will see the graphical user interface start and the Linux startup screen will display. The startup process can be monitored by observing the progress indicator bar on the startup screen as shown in Figure 5.

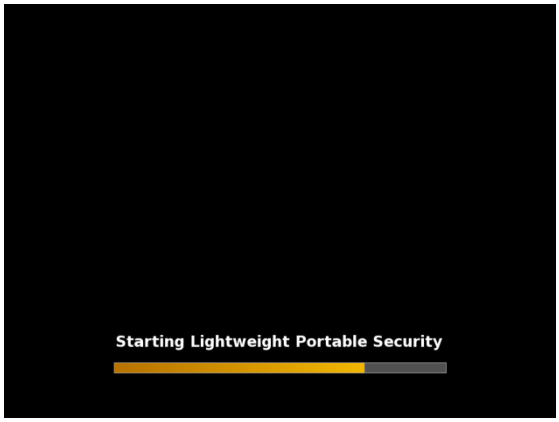

Figure 5 — Startup Screen

Pressing F2 during startup will display additional status messages as individual processes launch. However, this screen is optional and the information displayed is typically only used for debugging purposes and is of little use to most users.

Once LPS is loaded, the user session is initialized, and all startup messages are displayed, the graphical desktop will load and you may begin to use LPS. The startup device will not be mounted. Remove the CD or USB stick from your computer.

3.4 Boot Messages

If all goes well during the boot process described in Section 3.3, the local session will be initialized and LPS will be available for use. However, if there are exceptions during the startup process, additional messages may be displayed.

Once LPS is booted, but before it is available to use, the user will be prompted to accept the User Agreement, as shown in Figure 6.

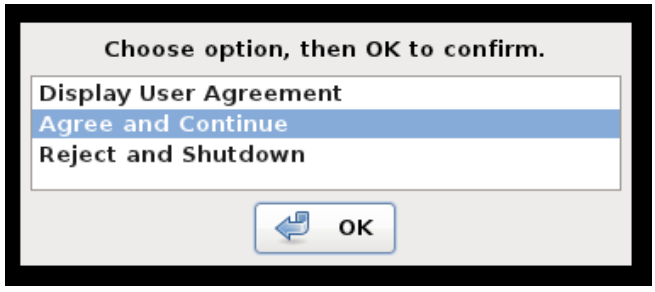

Figure 6 — LPS User Agreement Dialog Box

If the user agreement is accepted, the loading process will continue and the LPS desktop will be presented.

If the user agreement is rejected, the loading process will stop, the LPS disc will be ejected or the USB stick will be unmounted, and the computer will shut down. If you choose the option to display the User Agreement, you will be presented with the screen as shown in Figure 7.

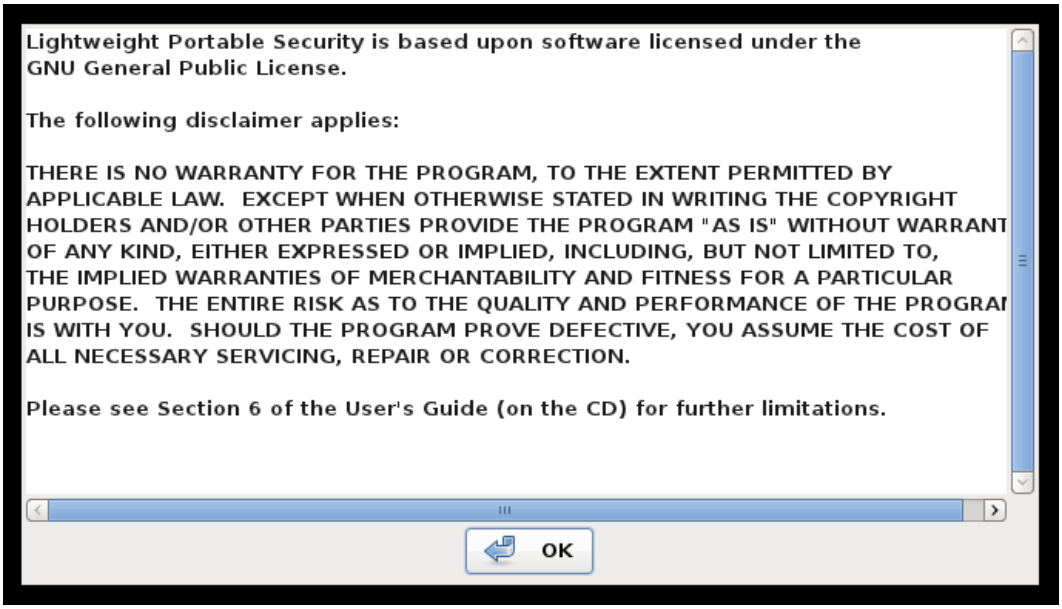

Figure 7 — LPS User Agreement

Once all startup messages are displayed, the graphical desktop will load and you may begin to use LPS. The startup volume (CD or USB stick) will not be mounted. Remove the CD or USB stick from your computer.

If LPS does not detect an attached smart card reader, a message similar to Figure 8 will display. This means that you will be unable to visit PKI-enabled websites until a smart card reader is connected. You can connect the reader at any time, but if you have Firefox open, you will have to restart the browser.

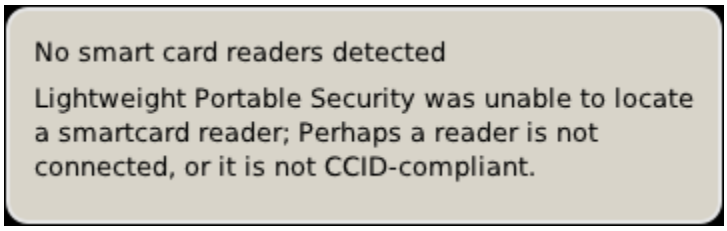

Figure 8 — Smartcard Reader Not Detected

4 Using LPS

LPS-Public is our flagship product and contains core features most needed by the widest range of our customers. We do create custom builds for specific organizations, so not all features and screens described in this guide will be the same in all distributions.

4.1 The LPS Desktop

Once the startup process finishes, you will be presented with either the LPS-Public desktop shown in Figure 9 or the LPS-Public Deluxe desktop shown in Figure 10.

Figure 9 — LPS-Public Desktop

This is the LPS-Public desktop environment. This desktop contains icons for:

- Firefox — a popular web browser with smart card, Java, and Flash support, and several useful add-ons.
- Encryption Wizard — AFRL's file encryption program.
- User's Guide — this document.

Optional icons that only are present under certain circumstances:

- LibreOffice — only available in LPS-Public Deluxe, this is the starting point for opening LibreOffice applications, which allows Microsoft Office files to be read and edited.

The status bar at the bottom of the screen has several areas containing useful utilities and information.

- The Start Button provides quick access to the same programs shown as icons on the desktop, plus these additional programs, utilities, and options to manage the LPS session:
    - Adobe Reader — a PDF file viewer that allows PDF forms to be digitally signed using smart cards (LPS-Public Deluxe only).
    - PDF Viewer — the eVince PDF file viewer (LPS-Public only).

- Secure Email — Thunderbird and DAVmail for performing S/MIME email functions, such as signing and encrypting email (LPS-Public Deluxe only).
- The *Configuration* folder contains various programs for adjusting system settings:
  - Date and Time — a utility for changing the current date and time settings, including the time zone.
  - Desktop Settings — a utility for changing font sizes and other cosmetic interface settings.
  - Display Properties — a utility to change the screen resolution, or adjust output to projectors or multiple screens.
  - Java — control center for Java preferences and security settings
  - Keyboard — a utility for adjusting input device preferences.
  - Mouse — a utility for adjusting input device preferences.
  - Power Management — a utility for changing preferences for when the system is connected to AC or battery power.
  - Printer Administration — a graphical utility for creating and managing print queues.
- The *Connectivity* folder contains networking utilities:
  - Citrix Receiver — the Citrix Receiver client, allowing connection to Citrix servers using the ICA protocol.
  - Instant Messaging — the Pidgin instant messaging client, supporting multiple protocols (LPS-Public Deluxe only).
  - Minicom Terminal Emulator — the minicom serial port VT102 terminal emulator.
  - Network Proxy — a utility for changing network proxy settings.
  - Ping — the multiping utility for testing network and host connections.
  - PuTTY — a graphical utility for connecting to local and remote terminal sessions.
  - Remote Desktop — the FreeRDP client, which allows connection to Microsoft Windows servers using the RDP protocol.
  - SSH — the OpenSSH secure shell client, used for remote command line access to host computers.
  - VMware View Client — the VMware Horizon View client, which allows connection to VMware View remote desktop servers using the PCoIP protocol.
- The *Debug* folder contains some troubleshooting tools that should only be run at the direction of LPS support personnel:

        - Debug Secure E-mail — a debug version of the Secure E-mail application. Do not run this version unless an error has occurred with the normal Secure E-mail application. This version creates additional log files which can consume disk space rapidly. Run the debug version of the program until you experience the failure condition, exist the program, then run the diagnostics utility to save the log files for support personnel.
        - Diagnostics — system logs and a detailed device listing useful for support personnel. LPS support personnel may ask you to run this utility and send them the output. No user-visible information is created running this utility.
        - Task Manager — a utility for stopping or restarting processes, which is useful if a program should stop functioning but not quit. It should not be used during normal operation since stopping processes may cause LPS to stop functioning correctly. If this occurs, reboot to start a clean session.
    - The *Documentation* folder contains online documentation:
        - About LPS — the "about box" describing the program and providing basic system information (Linux kernel version, available memory).
        - Encryption Wizard User's Manual — user's guide to the Encryption Wizard file encryption product.
        - README — online documentation for LPS, including disc labels, data sheets, and other information.
        - Release Notes — changes made in each product release.
        - User's Guide — this document.
    - The *Multimedia* folder contains various sound and graphics utility programs:
        - Media Player — a utility for playing videos or music (LPS-Public Deluxe only).
        - Sound Mixer — a utility controlling the volume of various audio outputs, including speakers and headphones.
        - Sound Properties — a utility for selecting and configuring audio and video devices and options.
    - The *Security* folder contains various security-related utility programs:
        - Check for OpenDNS — A tool for validating that OpenDNS is being used for DNS lookups.
        - Enable DNSCrypt — Encrypts DNS traffic and uses the OpenDNS service for DNS lookups, preventing some DNS-based attacks and increasing privacy. This feature is disabled by default, and must be enabled during each session.
    - The *Utilities* folder contains various utility programs:
        - Calculator — galculator, a basic desktop calculator.

        - CD Burning — utility for writing data to CD and DVD media.
        - Character Map — charmap utility, allows special characters to be selected.
        - File Manager — a GUI-based file browser (Thunar).
        - Image Viewer — the gpicview image viewer.
        - Onscreen Keyboard — a software virtual keyboard to allow data input without using a physical keyboard.
        - Paint — mtPaint, a graphics file editor.
        - SCR Firmware Update — a utility for updating SCM reader firmware.
        - Terminal Emulator — a terminal emulator for the X Window System (provides local command line access to Linux).
        - Text Editor — the Leafpad text editor.
        - UnZip — file roller utility, an archive manager for compressed files.
    - The *Shutdown* folder contains options to Shutdown and Reboot the computer.
- The Open Programs area shows any running programs or open windows. This area is empty if no programs are running and no windows are open.
- The Status area shows important system status indicators:
    - The Sound icon, which allows the sound volume to be adjusted.
    - The Network Manager icon, which serves multiple purposes:
        - The icon shows network status (disconnected, connecting, connected) and the type of connection (wired, WiFi, cellular broadband).
        - Hovering over the icon shows details about the connection status.
        - Left-clicking on the icon allows available connections to be established, or existing connections to be disconnected.
        - Right-clicking on the icon allows the utility to be configured (rarely used).
    - Battery icon, which shows the charging status and current charge of the laptop battery (computers with batteries only).
    - The system clock.

Figure 10 — LPS-Public Deluxe Desktop

4.2 Connecting to the Network

LPS supports wired, wireless (WiFi), and cellular broadband networking, but not dialup. We recommend using LPS with networks that use DHCP. LPS does not preserve user configuration data across reboots, so any static addressing information will have to be re-entered every time it is used. Likewise, wireless keys will also not be preserved between sessions.

Understanding the Connection Status Displays

The Network Manager utility in LPS manages connections via available network ports. If Network Manager detects an active port that has been configured to connect automatically, it will attempt to do so after LPS starts up. Otherwise, the network connection indicators will display when a manual connection attempt is made. Figure 11 shows the icons where the connection is in progress (grey) and the connection has been made (green).

Figure 11 — Connection in Progress Icons

Once a network connection has successfully been established, a temporary dialog box will display as is shown in Figure 12. The dialog boxes will automatically dismiss after a brief countdown.

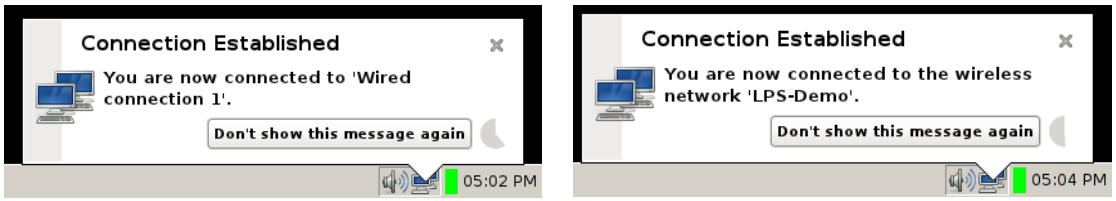

Figure 12 — Successful Connection

Once connected, the Network Manager status indicators will be displayed as shown in Figure 13. There are different icons for wired, WiFi and cellular broadband connections. Note how the cellular broadband status icon displays the signal strength. The WiFi display is similar.

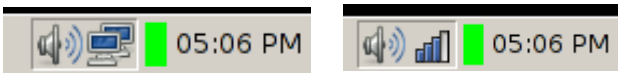

Figure 13 — Active Connection Indicators

Hovering over the active connection icons will show additional information, as shown in Figure 14. The information displayed will change based on the type of connection. Note how the cellular broadband status message displays the signal strength (WiFi is similar).

Figure 14 — Active Connection Detailed Information

Any active network connections can be disconnected by left-clicking on the Network Manager icon and then selecting the active connection to disconnect. Once this operation has been completed, the status change will be confirmed via a dialog box and network manager icon as shown in Figure 15. If LPS boots and does not find a working automatic connection, the Network Manager icon will display as disconnected (X in the icon).

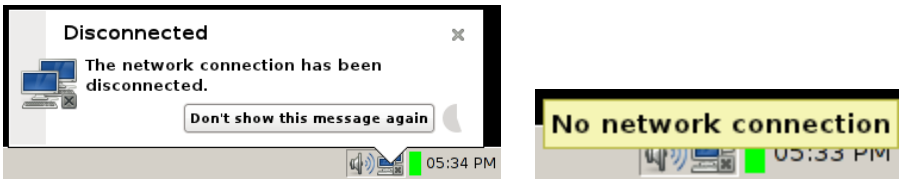

Figure 15 — Disconnected Status Indicators

Using Static Addresses on Wired Connections

It is possible to configure your computer to use a static IP address, but that requires some extra effort using the Network Manager utility. Right-click on the Network Manager icon in the status bar, as shown in Figure 16, then select *Edit Connections…*

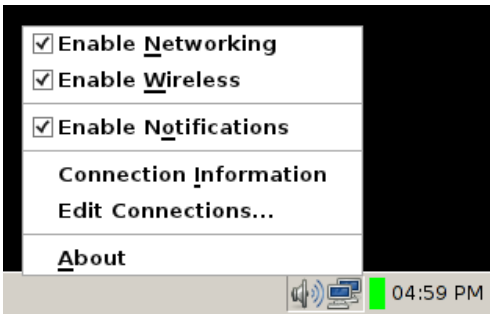

Figure 16 — Edit Connections in Network Manager

The Network Connections dialog will display. Ensure the *Wired* tab is selected, then click the *Add* button as shown in Figure 17.

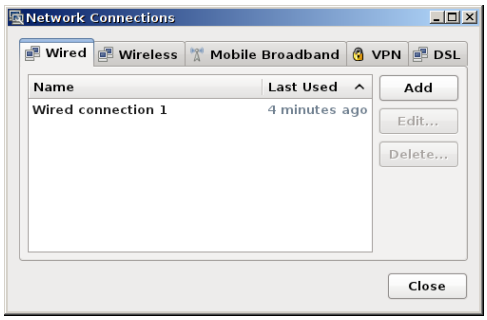

Figure 17 — Adding a New Wired Connection

The Editing Wired Connection dialog box will display. Select the *IPv4 Settings* tab, then use the drop-down box labeled ‘Method’ to select the *Manual* setting as shown in Figure 18.

Figure 18 — Selecting a Manual IP Configuration

Click the *Add* button, which creates an empty static IP address entry. Click on each field (address, netmask, gateway) as shown in Figure 19. Enter manual DNS settings if necessary.

Figure 19 — Setting Static IP Address

When finished adding the manual connection data, click the *Apply* button. The Network Connection dialog will now show that your new static connection has been defined (see Figure 20). This dialog box will also allow the definition to be edited or deleted. Click the *Close* button.

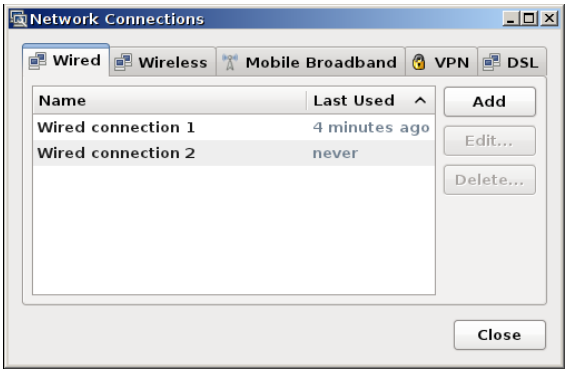

Figure 20 — Successful Static IP Address Created

Once the static connection is defined, you may have to manually initiate the connection. Left-click on the Network Manager icon in the status bar and then select the connection just created as shown in Figure 21.

Figure 21 — Initiating a Static IP Connection

The connection attempt will now be made, providing feedback via dialog boxes and status indicators as described in the previous section, *Understanding the Connection Status Displays.*

Using Wired Networks

If your computer was connected to a wired network port while LPS was booting, your computer should have an IP address assigned automatically by DHCP. If not, unplug your connection and re-insert your network cable to get a new address assigned. You can tell you are connected by observing the Network Manager icon in the status bar as described in the section *the Connection Status Displays.*

Using Wireless Networks

If you intend to use wireless networking (WiFi), start by left-clicking on the Network Manager icon in the status bar. You should see a list of available wireless networks detectable by your computer (see Figure 22). Select an available network to connect to it. If you need to connect to a

hidden network, select *Connect to Hidden Wireless Network…* and enter the appropriate network name. Note: wireless network names (SSIDs) are case-sensitive.

Figure 22 — Available Wireless Networks

Networks are displayed in alphabetical order. Note the indication of network signal strength (more blue bars indicates a stronger signal) and the network security status (a gold lock indicates that the network is encrypted and requires authentication). If you connect to a protected network, you will be prompted to enter the security credentials as shown in Figure 23. Select the appropriate wireless security method, enter the wireless password, and click the *Connect* button.

Figure 23 — Wireless Authentication Dialog

Depending on the type of encryption used, the key may be a hex string, a passphrase, or something more complicated. Most home and hotel networks will either be unsecured (not a recommended solution) or will use WEP or WPA. WPA2-Personal is the more secure option currently, but not all home devices support this protocol.

Using Cellular Broadband Networks

Initiate a cellular broadband network connection in the same manner as other connections: left-click on the Network Manager icon in the status bar. If LPS has recognized your cellular broadband modem, you will see a section called ‘Mobile Broadband’ with available connections under it. In the example shown in Figure 24, a Verizon card using CDMA technology has been selected. Other technologies may be displayed differently. Select the *New Mobile Broadband connection…* item to start the connection wizard application.

Figure 24 — Initiate Cellular Broadband Connection

The next screen to be displayed (Figure 25) simply describes the information that must be supplied to the connection wizard to initiate the connection. The screens may vary based on provider and cellular technology used. Click the *Forward* button to proceed.

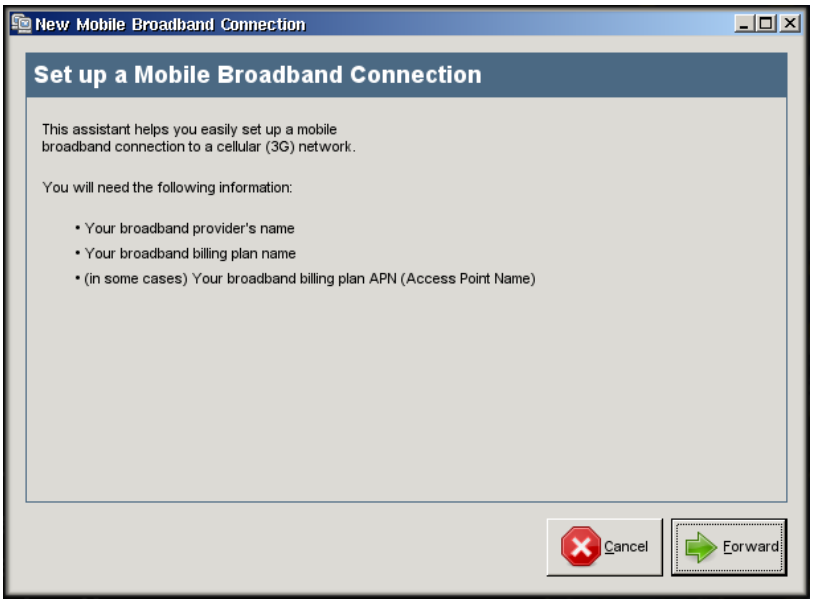

Figure 25 — Setup Cellular Broadband Connection

The next step is to select your cellular provider's country, as shown in Figure 26. The *United States* should be selected by default. Click the *Forward* button to proceed.

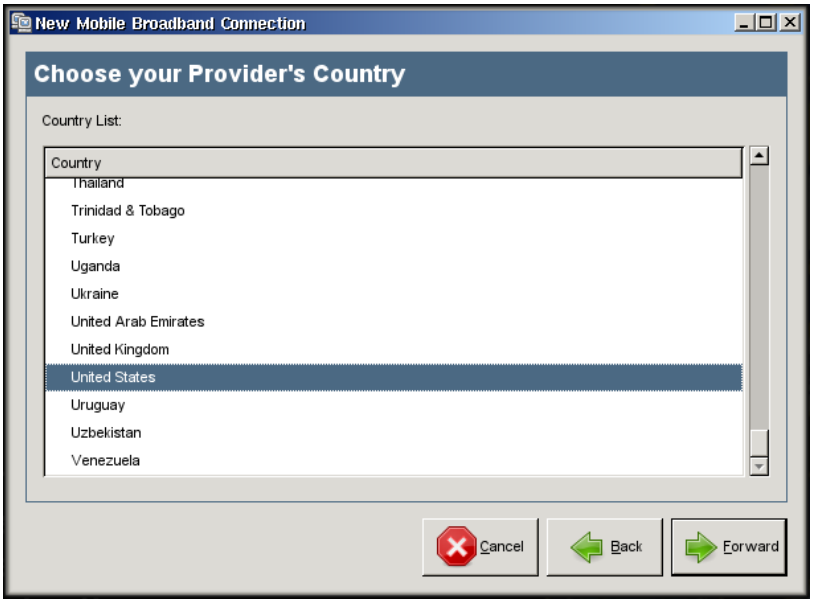

Figure 26 — Select Cellular Broadband Country

The next screen to be displayed allows you to select your cellular provider. Figure 27 shows the listing for the United States. Choose your provider and click the *Forward* button to proceed.

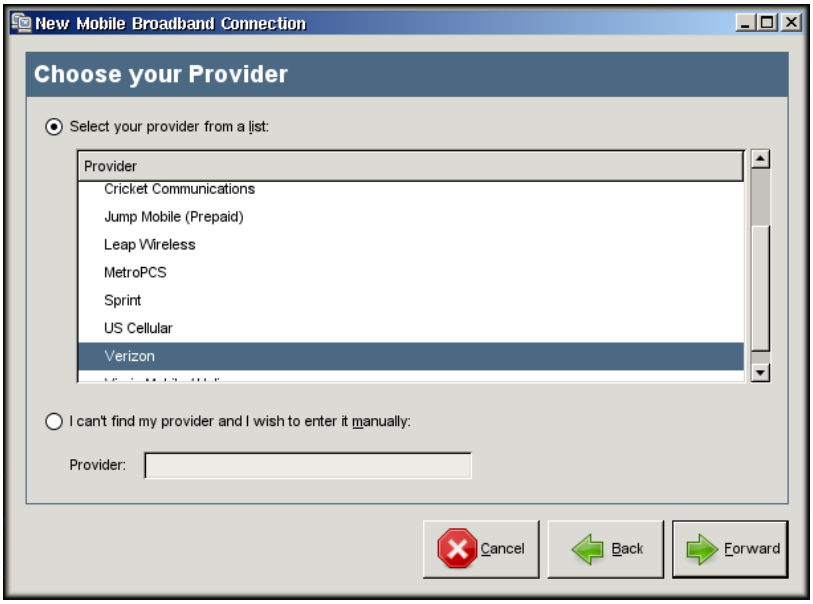

Figure 27 — Select Cellular Broadband Provider

The final screen shown in Figure 28 summarizes the selections made on previous screens. Click the Apply button to accept these choices and proceed with initiating the connection. The connection status will be shown as described in the section on *Understanding the Connection Status Displays*.

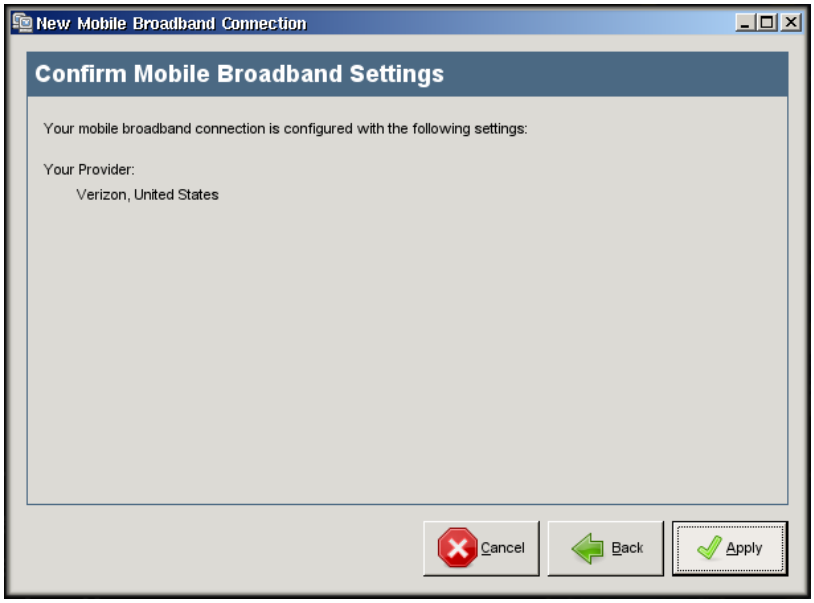

Figure 28 — Complete Cellular Broadband Connection

Cellular broadband networking support is a relatively new feature in LPS, so not all devices may be supported. If your device is not detected, be sure to let us know so we can investigate adding support to a future release.

Using iPhone Tethering

LPS now supports tethering Apple iPhones, which allows an iPhone with an appropriate tethering plan to be used as a cellular broadband modem. LPS detects the iPhone as a wired Ethernet device, displaying "Wired Network (Apple iPhone)" in the Network Manager display (Figure 29). If auto-detected, the iPhone will usually appear as the "Auto eth2" device (assuming the system has only one other wired network controller).

Figure 29 — Successful iPhone Tethering

LPS should connect automatically when booted with an iPhone tethered to a USB port. If not, disconnect the iPhone and reconnect it. Verify that the iPhone is displaying a dark blue "Personal Hotspot" (as shown in Figure 30) overlay across the top of the iPhone display. iPhones running iOS 4.3 or later will use "Personal Hotspot," while older phones will use "Internet Tethering." iPhone tethering on LPS has only been tested with USB-connected iPhones; some iPhones (iPhone 4 and later) support WiFi tethering.

Figure 30 — iPhone Display with Tethering Enabled

iPhones must be configured to support the Personal Hotspot feature using the Settings app. A valid tethering data plan must be purchased in order to use this feature. Contact your wireless service provider for more information. If the iPhone is not displaying the Personal Hotspot overlay, then the iPhone is not functioning as a cellular broadband modem.

If the iPhone is displaying the Personal Hotspot overlay, but no network connection exists. Try initiating the connection manually. Click on the Network Manager icon, and select the "Auto eth2" connection (or similar entry under "Apple iPhone") as shown in Figure 29. Observe the status indicators as described in the *Understanding the Connection Status Displays* section.

4.3 Browsing the Internet

Use the Network Manager to initially verify connectivity; look at the status icon as described in Section 4.2. Start up the Firefox web browser and test basic network connectivity. Browse to a public website like *www.google.com*. If you are accessing the network from a hotel or other public location, there may be intermediate network access screens to navigate. For example, some hotels and public Internet cafes require entering codes or acknowledging licensing agreements before granting access to the public Internet. If your networking does not work properly, see the troubleshooting discussion in Section 6.

The standard LPS-Public distribution includes the Firefox web browser. Starting the Firefox application should be sufficient to start browsing the public Internet. Some custom LPS distributions may have the default browser removed. In that case, connect to an enterprise network using a VPN, remote desktop or terminal server application and browse from within the target network.

Once basic network connectivity is verified, you can use LPS applications to connect to private networks using a variety of protocols. LPS can support several different methods, and not all may be present in your specific LPS distribution. Check with your network administrators or computer support staff to determine the best method for connecting to your private network.

LPS does not impose any restrictions on what sites you can visit, but it also won't bypass any firewall rules, proxy servers, or other filtering and control restrictions in place on whatever

network you are using. Some organizations have corporate policies blocking access to certain websites from within their networks. In that case, the browsing experience could be different when connected to the corporate network than when using the browser directly within LPS.

4.4 Using a Smart Card

Government users in the DoD are familiar with using the Common Access Card (CAC) to authenticate to computer systems. Other US Government users are familiar with using the Personal Identity Verification (PIV) card for the same purpose. LPS supports using an external USB smart card reader, but not as many internal readers. Make sure the smart card reader is connected to the computer and be sure the smart card is inserted before launching the web browser. This allows the use of PKI-enabled websites.

If you access a PKI-enabled website, you will be prompted for a certificate. CACs and PIVs typically have multiple certificates loaded. In the User Identification Request dialog box, you will be prompted to select the appropriate certificate. Choose a certificate from the drop-down list—it is typically the ID certificate on the CAC/PIV, although some web applications, particularly Outlook Web Access (OWA), can use the Email Signature certificate for validation (see Figure 31).

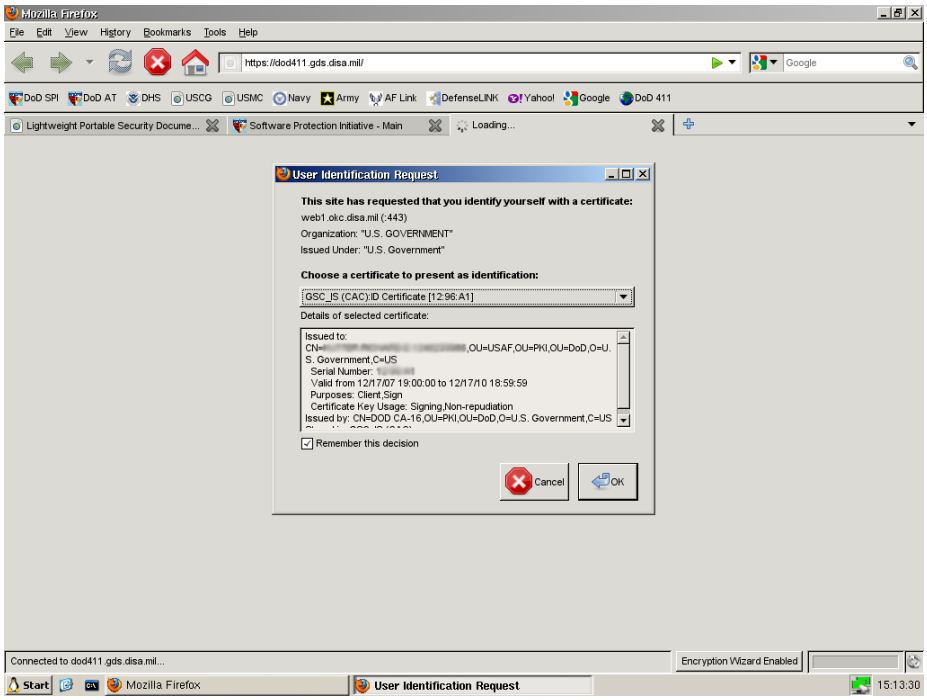

Figure 31 — Certificate Selection

You will next be prompted for a password (the Password Required dialog box—See Figure 32). It requests a Master Password, which is simply your PIN.

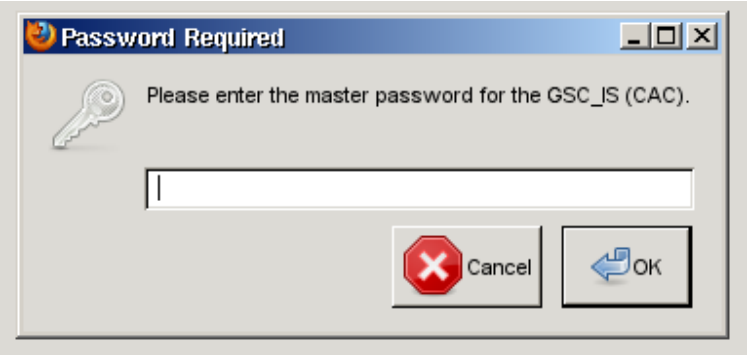

Figure 32 — CAC PIN Request from Firefox

Subsequent web pages and application may request further authentication (either CAC/PIV or username/password). Continue to supply your PIN or credentials when requested.

4.5 Using Email

You may have several different email accounts—from corporate to personal—that you want to access while running LPS. The experience will vary based on specific customizations within LPS, but the standard distribution will allow you to check private email (e.g., gmail) via a web interface, corporate email via a web portal, corporate email via remote desktop services, and potentially host-based email via ssh.

To connect to email, you first have to understand where the system is running. If you are using a web-based commercial service, then simply connect to the Internet, start Firefox, and connect to your email service. Supplying typical username and password credentials will give you access, and all operations are performed from within the browser.

If you are using a corporate or private email solution, then you will have to determine whether you are connecting to it via a web portal or via remote desktop services. A private email system will often support both interfaces. To use a web portal (e.g., OWA), you will have to establish a secure web connection (*https:* not *http:*) to a webmail server. Your email administrators will provide you with the URL for the server, and any login instructions. Authenticating to most US Government email services requires the use of a smart card; other solutions may require a simple username and password. LPS supports two methods for accessing OWA-based email, OWA through the Firefox web browser and DAVmail using Thunderbird, as described in the "Using OWA" section below.

Another popular solution for corporate or private email systems is to use a remote desktop or application virtualization solution (e.g., Citrix) to access either a full desktop or an application on a remote system. In the full remote desktop solution, the client presents a virtual desktop that is running on the corporate or private network. Screen images, not data, are being transferred between the client and the server. The server is manipulating the data on the private network on your behalf. Once in a familiar desktop, you can run a variety of applications including an email client (e.g., Outlook). This solution is popular since it presents a familiar interface and uses the same software as would be used if you were directly running on the private network. Application virtualization is similar, except a specific application is presented rather than a full desktop. Running the email client as an application would give you the same email experience as from the desktop virtualization solution, except that you wouldn't be able to run other applications.

Some people using host-based email solutions might use ssh to access the remote system. Supplying a network address and credentials allows host-based access where email applications can be run. Similarly, remote desktop software allows access to other systems where applications can be run, but are generally done within the same network.

Using OWA

OWA is the web-based interface to Microsoft Exchange server. It means 'Outlook Web Access' in every version of Exchange through version 2007, and 'Outlook Web App' starting in Exchange 2010. Since it means different things depending on the version, it's best to just refer to it as OWA.

A webmail session is started by launching the Firefox web browser. Enter the URL of the OWA server given to you by your organization. The OWA authentication screen will require either a username and password or smart card certificate and PIN, depending on how it is configured. Assuming you are using a smart card, select the correct certificate (typically the Email Signature Certificate), and then provide your smart card PIN. This is the same process described in Section 4.4.

The OWA interface looks and acts differently based on the version of Microsoft Exchange running on the server. Newer versions usually have a cleaner interface and more capability, but all will have basic functions that allow you to read and send normal email.

In current releases of Microsoft Exchange (verified through Exchange 2010), Microsoft uses a proprietary interface for signing and encrypting email. This means that clients not running on a Microsoft operating system using a Microsoft browser will be unable to perform these functions. Signed emails can be read, but not created. Encrypted email cannot be read or created.

Using Secure Email (DAVmail/Thunderbird)

DAVmail and Thunderbird are an alternative to using OWA that can often support the digital signature and encryption features that OWA does not provide on non-Microsoft clients. Thunderbird is an email application that runs on LPS, and DAVmail is a software gateway that sits between Thunderbird on the client and an Exchange/OWA server. A gateway performs protocol and format translations, but is an extra step between systems that causes a performance penalty for every operation. Understanding how to properly use Thunderbird and DAVmail can make this experience much easier to bear.

To use DAVmail/Thunderbird, launch the **Secure Email** application in LPS under the Start button.

The DAVmail/Thunderbird setup dialog box appears, as shown in Figure 33. Several fields must be input correctly in order to use the solution:

- Enter email address – use a full email address that works for you on the system to which you are connecting. It does not have to be your primary email address; aliases work, as long as they can be used to receive mail.
- Select server – leave as Custom if the drop-down box is not pre-populated.
- Uses Smart Card (CAC) – leave this box checked if you are authenticating with a smart card.

- If Uses Smart Card (CAC) is unchecked, you have the option of entering a different username for login purposes (if the login name is different than the email address, which is not typical)

- Use DoD LDAP – leave this box checked if you want to look up addresses and digital certificates from a DoD directory service. Note that a valid DoD CAC is required to use this service.
- Change Dates – click this button to change the date range; the default is 3 days before today. You have two options, On This Date (selects email from one day only), and Since This Date (selects email from that date to today).

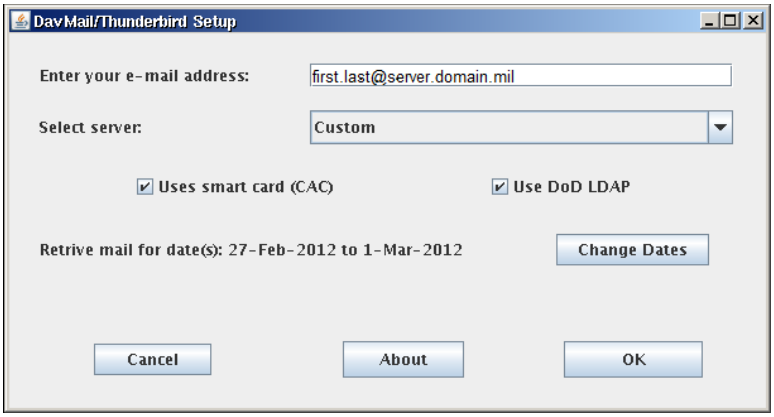

Figure 33 — Email Setup Dialog

Once the fields have been entered properly, click the OK button (it will be greyed out until necessary fields have been entered – if you have entered data and it is still grey, hit the TAB key to exit the field).

A popup dialog will display to allow you to enter the URL of your OWA server. Enter a complete address, including the "https://" and click OK. This dialog is shown in Figure 34.

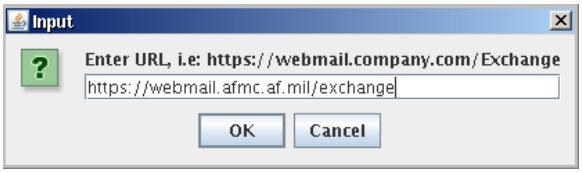

Figure 34 — OWA URL Input Dialog

You may see a popup (Figure 35) in the lower right corner of your screen as the DavMail Gateway program launches – this is normal.

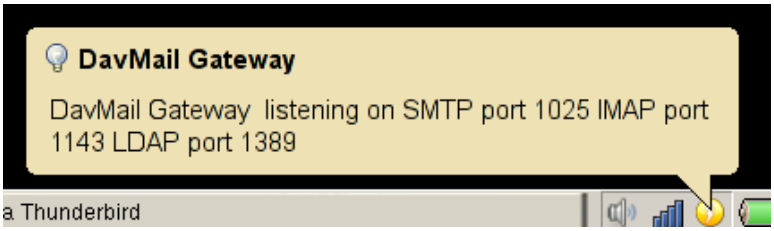

Figure 35 — DavMail Gateway Launch Message

You will also get another popup asking you to confirm that your smart card is inserted; click OK. The Thunderbird email client will now launch while the DavMail Gateway negotiates access to your server-based email. You will have to enter additional information so that DAVmail can authenticate you to your mail server. You will first be prompted for your smart card PIN, and then you will have to select the proper certificate for authentication – dialogs for these operations are shown in Figure 36. The certificate to choose depends on your mail system, but most will commonly use the Email Signature Certificate.

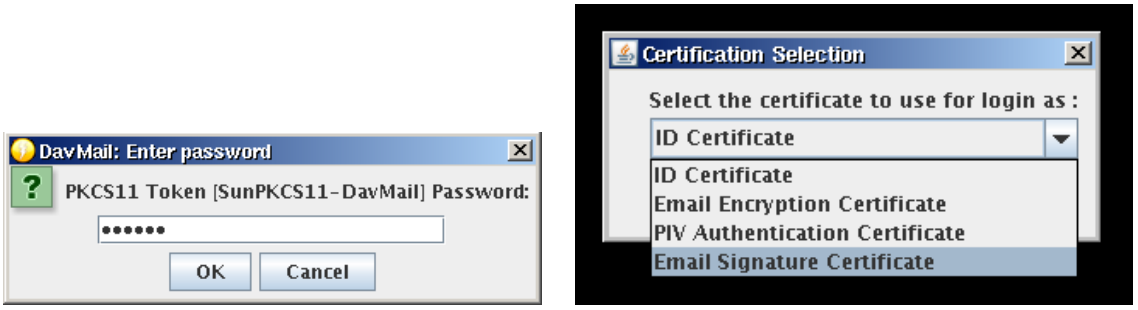

Figure 36 — DavMail PIN Entry and Certificate Selection

Watch the Thunderbird status bar at the bottom of the screen; status messages will be displayed. You will see messages like "Sending login information…" and "Looking for folders…" These are correct messages; if there are errors, they will be displayed in the status bar or in DAVmail popup messages. The Thunderbird progress bar (lower right hand corner of window) will also be moving while network activity is in progress.

The Thunderbird client will be active while your login information is validated, the folder list is populated, and message headers are downloaded. The status bar will show information like "INBOX Downloading message header 12 of 54" while this is taking place (see Figure 37). Once all message headers are downloaded, you can start using the program. Please wait for all messages to download!

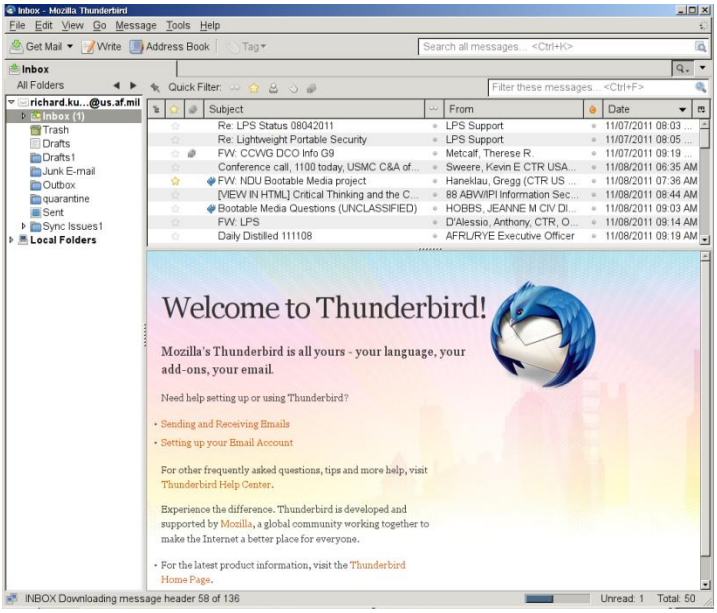

Figure 37 — Thunderbird Client with Message Headers Downloading

If Thunderbird opened a "What's New in Thunderbird" tab, you can close this window. If you don't start automatically in your inbox, click on your mailbox name in the left window pane, expand the selection, and choose your inbox. You will see a list of message headers in the upper navigation pane. Any selected messages are displayed in the lower reading pane.

Performing Common Email Tasks using Thunderbird/DAVmail

Reading a Message. Select a message header in the upper navigation pane to start the download of the full message. Watch the status on the bottom of the screen as the message downloads. The message will display in the lower reading pane.

Reading an Encrypted Message. The process is similar to reading an unencrypted message, except that you will be prompted to enter your smart card PIN. If the sender has encrypted the message properly using your public encryption certificate, the message will be decrypted and displayed.

Creating a New Message. Click the 'Write' button in the Thunderbird icon bar at the top of the main window. Enter the SMTP address of the recipient (no internal address books are included). Click the 'Send' button when done. Messages created within Thunderbird are signed by default.

Creating an Encrypted Message. First, you need to know the correct SMTP address of the recipient. The important point is that the address needs to be *the same one that is used on their Email Encryption Certificate*, which may be different than their "normal" email address. If you don't know this, you may need to look it up using DOD411 or DOD Enterprise Whitepages.

In the 'To' field, enter the email address. Use the Security dropdown to sign, encrypt, or both. Click on the Security button to validate the certificate of the email recipient. Enter the body of your message. When done, select the Classification status and then click the SEND button.

During this process, you may be prompted for credentials when looking up the certificate. This will also happen when you click the Security button after entering an email address. The dialog will say User Identification Request; it is prompting for your certificate – select the ID Certificate. In the Password Required dialog, enter your CAC PIN. Depending on network speed, you may see a message saying "Downloading certificates."

When the recipient's certificate has been downloaded, look for the status of the certificate. If it has been found and is ready to use, the status will say 'valid'. If the email address is incorrect (usually that it isn't the same as on the certificate), the status will say 'not found'.

This imports a user's encryption certificate into your address book. You can now use it for messaging purposes, including addressing and encryption.

In some environments, this automated process does not work. However, there is a workaround that can be used. The important thing to remember is that if you want to work with encrypted messages, you need to have the other party's encryption certificate downloaded to your computer and put into your address book.

The manual process for looking up an encryption certificate is:

- Start Firefox
- Use the DOD Whitepages browser bookmark
- Authenticate to the DOD Whitepages site

- Enter search criteria to find the other person
- Click on the record for that person
- Click on 'Download Certificate'
- Save the file to your computer; it will be of the form <name>.cer. The default location will be /home/ts/Downloads/<name>.cer.
- In Firefox, navigate to the cert import function (it's kind of complicated):
    - Edit/Preferences
    - Advanced (icon)
    - Certificates (tab)
    - View Certificates (button)
    - People (tab)
    - Import (button)
    - Open [select the path where you saved the .cer file]
- You can verify that it worked by looking for the person in your local address book. You can use this contact to both address emails and to encrypt/decrypt emails.

This manual process can be used for any number of recipients. Once you have populated your address book with the contacts you will use, the encryption process proceeds much more smoothly.

Using Defense Enterprise Email

Defense Enterprise Email (DEE) is an enterprise-wide email service used within the DoD. It can only be accessed using OWA, not Secure Email. DAVmail and Thunderbird require a VPN connection to access DEE; VPN is not provided in LPS-Public. An alternative is to have your organization request Bootable Media. Note that when using OWA, you will be unable to sign, encrypt, or decrypt messages due to Microsoft's lack of full support for non-Windows clients.

This restriction could also apply to other email systems that require a VPN to fully use OWA. If DAVmail is unable to establish a connection to your messaging server, this could be the reason.

Planning Your Email Use

Thunderbird has some advanced capabilities, but must use the DAVmail software gateway to communicate with a remote email server's web interface. This process is inherently slower than other methods, and can be frustrating to use when a large number of messages are downloaded. Following are some tips to help you use the email capabilities within LPS in a more productive way:

- Use OWA as your primary email interface, particularly to read AND DELETE email. Understand that you can read signed (but not encrypted) email and can send unsigned email using this method.

- Before performing tasks involving encrypted email, first clean out all unwanted messages from your inbox – this will reduce the number of messages which have to be downloaded by DAVmail. Note which messages are encrypted, and look at the date of the messages.
- When starting DAVmail, don't pick a date earlier than the earliest message you want to read. It takes much longer to download earlier messages. If you can just select the day of the message you want, use that option first.
- Use DAVmail to create encrypted mail. You will need to know the proper email address of the recipient. Select the Security dropdown button to choose the proper action, either "Encrypt this message" and/or "Digitally sign this message" – messages are signed by default.
- Use DAVmail when needing to create signed email. This is the default in the program.
- Use OWA to create normal (unsigned) email. It will be faster.
- In general, use OWA when you can, and only use DAVmail for the specific purposes where it has unique capabilities. If you try to use DAVmail to read all your email, you will have a slower experience. You can still use this method if you prefer, but if you experience performance problems, it is probably based on how you are using the program.
- Use directory services to lookup email addresses. You will not have a Global Address List on your computer, so you will need to use an external service. LPS has been pre-configured with the DOD411 service, which allows names and certificates to be queried. Using Firefox, browse to this service, and authenticate using your ID certificate and CAC PIN. Search by first and last name, locate the person you want, and note the email address used on the certificate. This may be a different email address than you typically use. If you are encrypting messages, you must use this address or you won't be able to find the appropriate encryption certificate.
- You may wish to keep Firefox open when using DAVmail/Thunderbird. Open a browser tab and authenticate to DOD411 or DOD Enterprise Whitepages using the provided browser link. Use this browser window as your address book when using the email application.

Email Usage Tips and Troubleshooting

- If DAVmail crashes or hangs, just restart the Secure Email program – the application will reload. Choose 'current' to reuse your last settings.
- Understand if your OWA servers (even if using Secure Email) are on the public Internet or on a private network. If on a private network that requires a VPN connection, LPS-Public will not work; Bootable Media must be used.
- When using OWA, if you click on a message and it doesn't display, it may say "The content can't be displayed because the S/MIME control isn't available." This means you are accessing an encrypted message – use Secure Email to read it, not OWA. The message should appear in OWA with a blue lock icon but it may not display properly if you are using Conversation view.

OWA, smart card certificate lookups, and Secure Email rely on external network services. These networks are not always available, and communication problems (especially slow networks) may cause intermittent failures. If you have a failure connecting to a remote system, try again several times. Try rebooting LPS to see if that helps. Attempt to verify if the remote services are active and responding.

4.6 Using Instant Messaging

The Pidgin Instant Messaging client is included with LPS-Deluxe only. This client allows you to interface with multiple popular Instant Messaging services.

Launch the Instant Messaging client from the Start menu. You will be presented with an Accounts screen, which allows you to configure the service. Once you have created an account, you will not see this screen. Once the service is running, you can access Instant Messaging by right-clicking on the icon between the network and battery icons in the status bar.

Click the 'Add' button to add a new account; the dialog shown in Figure 38. Start by selecting the Protocol from the drop-down list. This is either a public Instant Messaging service, such as Google Talk, Yahoo, AIM, or MSN, or a protocol to connect to an internal (non-public) service. Configuring the public services is very straightforward. Simply select the protocol, enter your credentials (username and password), and optionally other identifying information (such as a screen or display name). If the credentials are valid, you should see a Buddy List populated with your existing Instant Messaging contacts.

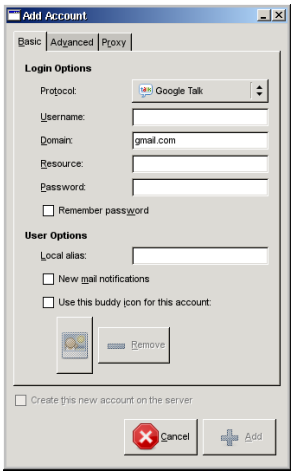

Figure 38 — Instant Messaging Add Account Dialog

If you add multiple accounts to Instant Messaging, your Buddy List will display all your contacts in a consolidated window. To start a conversation, double-click on a contact and type in the conversation dialog. To create a contact, use the Buddies/Add Buddy menu option in the Buddy List. You must know the username (email address) of the person you wish to invite.

4.7 Saving Your Work

By design, internal storage devices are not supported by LPS; this prevents malware from being stored and interfering with subsequent operations. LPS-Public supports the use of FAT, FAT32,

and NTFS formatted external storage devices (e.g., USB hard drives, flash drives) and read-only CD/DVD drives. This functionality may be removed in some custom versions of LPS.

LPS runs entirely in RAM without local storage devices. The initial filesystem loaded into memory comes from the boot CD. Any changes made to files or directories during the session will be lost upon reboot unless saved elsewhere. Users may not have permissions to write to most directories within the `/` (root) filesystem, so it's best to use the home directory (`/home/ts`) to save files temporarily. Note that if Firefox is used to download files, they go to the Downloads directory by default (`/home/ts/Downloads`). The amount of temporary storage available to users depends on the total amount of memory available in the computer; remember that LPS and its initial filesystem will consume some of this memory. Whatever left is available for working files during the session.

Users may download working files and work on them during the active session, but remember to move them to permanent storage before shutting down the system. Simply saving files to the local RAM disk will not keep them past reboots. Several options exist for permanently saving the working files, including saving to cloud-based storage (such as a SharePoint portal or another similar web-based file storage service within the Government network), emailing the files to yourself or to co-workers, or saving to removable media (e.g., USB hard drives, flash drives), if this functionality has not been disabled in your custom build. Note that network drive support is not enabled by default, and requires additional settings to use with smart card authentication.

Keep in mind the sensitivity of the data being saved when choosing the storage location. Do not post official Government files on public data storage networks unless authorized to do so by your computer security office. Some work may need to be encrypted prior to storage or transmission; Encryption Wizard can be used for this purpose (see Section 4.12). Always follow your organization's guidance on how to handle and store data.

When LPS-Public boots from a USB flash drive, the boot stick will be unmounted after LPS finishes loading. We recommend that you use separate boot and data flash sticks to protect your boot device from contamination. If you use LPS on a flash stick in the same way as on a CD (i.e., separating your boot device from your data storage device), you will be operating in a more secure manner.

You can connect external storage device to your computer before or after booting the system. LPS will recognize devices being connected and will mount them automatically. When you insert a USB device, an icon will show up on the desktop (see Figure 39). You can browse files on the device by left clicking on the icon or using the File Manager as shown in Figure 41.

Figure 39 — USB Device Mounted on Desktop

External USB devices are mounted in the Linux file system under `/media`. You can browse these volumes using the File Manager, the command line, or the Open and Save dialog boxes of applications such as Firefox, eVince, Adobe Reader and LibreOffice.

Before you unplug a USB device, right-click the USB device icon on the desktop as shown in Figure 40, then select ‘Unmount Volume’ or ‘Eject Volume’. A confirmation dialog will appear. The USB Device icon will disappear from the desktop when ejected.

Figure 40 — Safely Remove USB Storage

Using this utility ensures that all files are closed and the drive is unmounted cleanly.

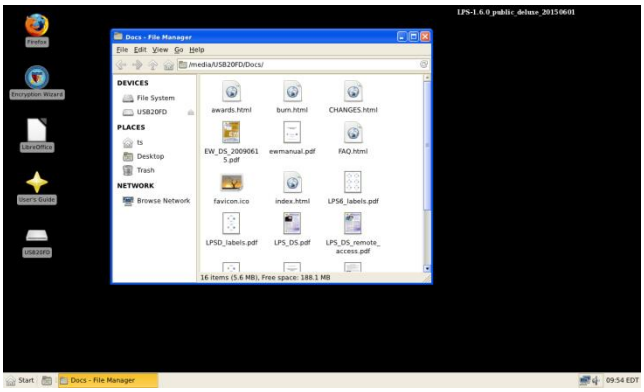

Figure 41 — USB Device Opened in File Manager

LPS also supports internal and external USB-connected CD and DVD drives for reading (but not writing) files. To use a CD from an external driver, connect a USB CD drive, power it on (if necessary), and insert a disc. The CD should be mounted on the desktop similar to a USB drive as shown in Figure 42.

Figure 42 — CD Mounted on Desktop

The disc will be mounted as /media/CDROM. Open the File Manager to browse the disc as shown in Figure 43.

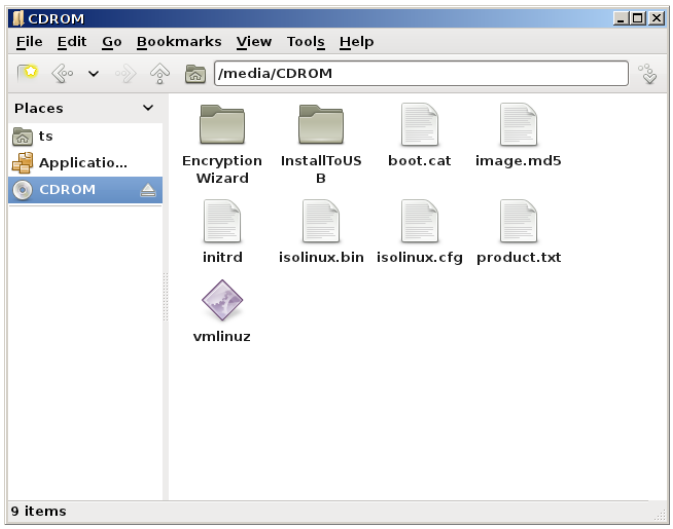

Figure 43 — Browsing a CD

As with USB drives, the disc can be ejected from the File Manager, or by right-clicking the CD icon in the system tray and selecting ‘eject cdrom’ as shown in Figure 44.

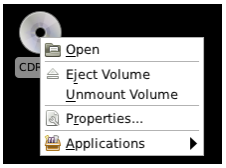

Figure 44 — Ejecting a CD

4.8 Working with Compressed Files

LPS has support for working with .zip and other compressed file archives. This feature is provided by standalone UnZip utility.

If you have downloaded a zip file, you can unzip it using the File Manager. Open the Downloads folder or launch the File Manager and browse to the directory containing the file. Left-click on the file to launch the UnZip tool and select Extract from the toolbar or the Archive menu. The files in the zip archive will be uncompressed in the designated directory.

You can create an archive using the standalone UnZip tool. Open the application (under the Start/Utilities menu), then either create a New archive (to make a zip file) or Open an existing archive (to unzip files).

4.9 Printing

LPS works with USB-attached printers and local network printers. To use a printer, a queue must first be established. Open the Printer Administration utility in the Utilities menu, as shown in Figure 45.

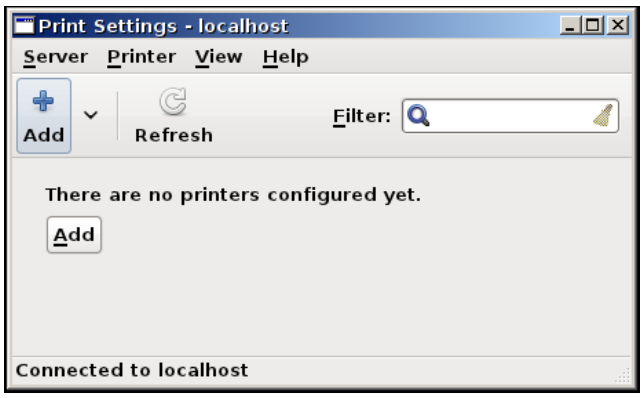

Figure 45 — Printer Administration Screen

If you have a locally-attached printer, it may be auto-detected. Check the Printer Administration screen to see if the queue has been established. If the printer is attached after LPS boots, a connection message will be displayed if it properly detected and configured, as shown in Figure 46. If your printer was detected and a queue established, you are ready to print.

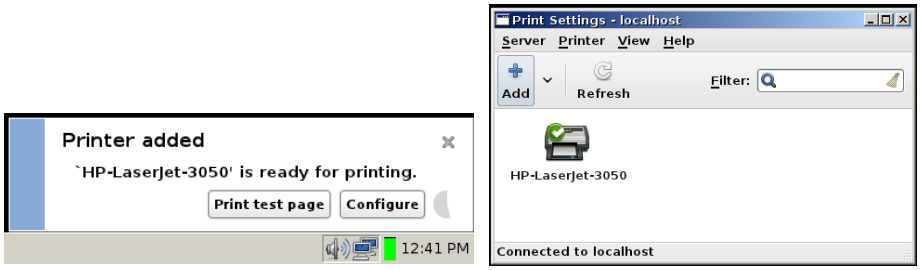

Figure 46 — Local Printer Detected

If you do not have a queue defined, follow these steps:

1. Click the *Add* button. The **Select Device** screen displays as shown.
2. Wait for the spinning wheel to stop; this is the utility detecting your local and network printers. The list of devices may update as devices are detected. You may need to expand the Network Printer line to see detected network printers.
    a. If your device is listed, select it and press the *Forward* button.
    b. If your network printer is not detected, enter the host name or IP address hosting the printer, then press the *Forward* button (Figure 47).

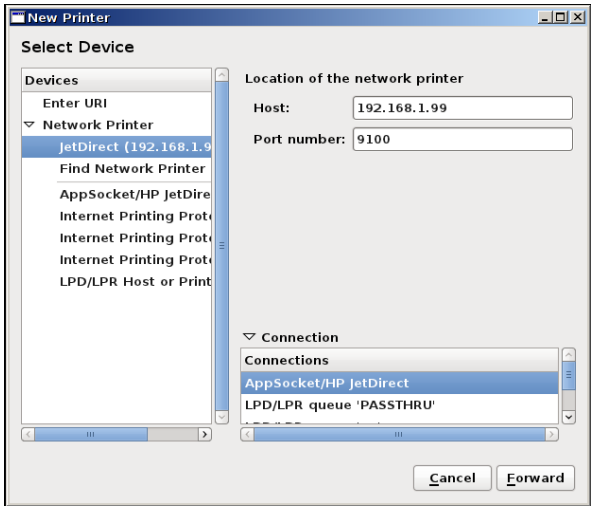

Figure 47 — Choosing a Network Printer

3. The Printer Administration utility will attempt to find a driver for the printer.
    a. If it finds one, the **Describe Printer** screen will display. Generally, the information will be correct so simply click the *Apply* button.
    b. If it doesn't, the **Choose Driver** screen will display. Select the Vendor of your printer, then select the model of your printer.

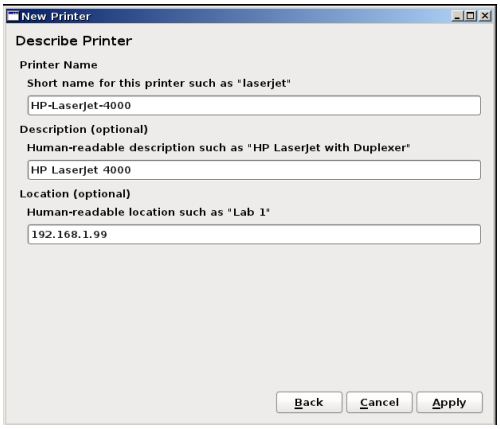

Figure 48 — Creating a Network Print Queue

If your model isn't listed, try choosing one with a similar number. Alternatively, select the Generic vendor and then either the PCL or Postscript driver for your printer, depending on the type of printer. Click the *Forward* button; the **Describe Printer** screen will display. Click the *Apply* button.

4. The print queue icon should appear in the Printer Administrator utility (Figure 49). Double-click on it to see the settings. You can use the Print Test Page button to test your printer, if desired.

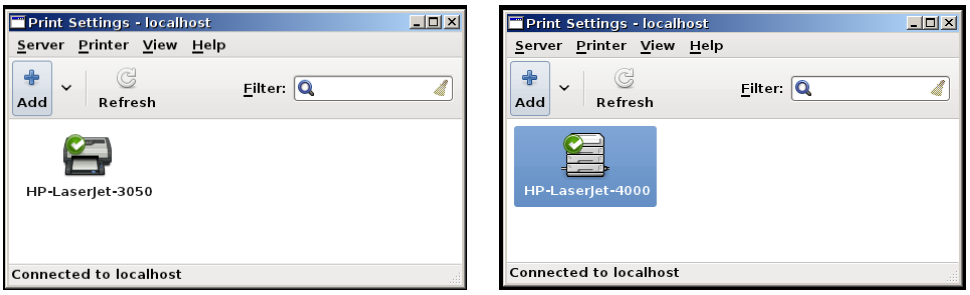

Figure 49 — Local and Network Print Queues Defined

5. If your printer doesn't work, you can right-click on the print queue then delete it, and then recreate the queue with different settings. Alternatively, you can right-click on the print queue, select *properties*, then click the *Change* button on the **Make and Model** line to select a new driver.

You should now be able to use your printer from within applications. Many applications have Print, Print Preview, and/or Page Setup menu commands that will allow a printer to be selected. You must have created the print queue via the Printer Administration utility before it can be used by an application.

You can view the contents of the print queue by selecting the queue, and using the Printer\View Print Queue menu command, or by right-clicking on the queue and choosing *View Print Queue*. The queue display is shown in Figure 50. By default, the queue listing shows active jobs unless the Show Completed Jobs button is selected.

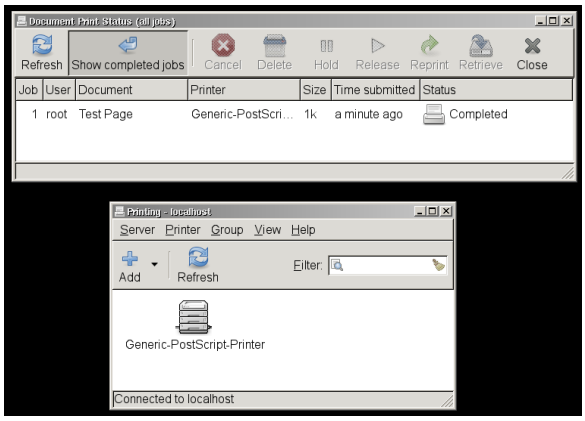

Figure 50 — Print Queue Status

4.10 Using DCS for Online Collaboration

LPS includes support for webcams meeting the USB Video Class (UVC) specification. UVC is a logo requirement for Windows Vista, so any webcams having a Windows Vista (or newer) logo on the box will likely work with LPS. Older webcams are unlikely to work with LPS. Applications or web sites with webcam support should be able to access the hardware directly.

Defense Collaboration Services (DCS) is a web service for DoD enterprise collaboration. Real time web conferencing software is used to have online meetings, including using desktop video

conferencing. Java and Flash are used to deliver the content, so these components must not be disabled in order to use DCS.

Following is an overview of how to access and use webcams in DCS meetings:

1. Open Firefox, and select the link to DCS under DoD/Collaboration. The DCS web page will appear. Accept the user agreement.
2. Under the *My reservations* section, click on *Create a new reservation*. Give it meeting name and description. Click on the meeting name under *My reservations*. Select the *Web Conference* tab to obtain the link to your web conference and forward to other attendees. Click **Start** to launch the meeting.
3. Attend a meeting created by another user by opening the URL to the web conference in the sent invitation.
4. Inside the meeting, first set up your microphone. Select the *Share My Microphone* headset icon in the upper left. If prompted with an Adobe Flash Player Settings dialog, select *Allow* to grant permission to use the microphone. Select *Test or Change Microphone* for configuration options and **Join Audio** to begin using your headset. DCS recommends using Join Audio only when you are about to speak.
5. Now set up your webcam. Select the *Share My Webcam icon in the upper left corner* . If prompted with an Adobe Flash Player Settings dialog, select *Allow* to grant permission to use the webcam. You should see input from your camera displayed on the screen. Select **Start** Sharing to make your image available to others. If you are collaborating with users with a webcam, you will be able to see them in the display as well.
6. When sharing your screen, Java may display a warning dialog requesting permission to run the BigBlueButton Deskshare Applet. You will need to select **Run** to proceed. When *Closing* screen sharing, you may need to **Allow** access to the applet.

DCS has extensive documentation online. See their user manuals and online training links on their main web page for more information about the application.

If you have trouble hearing sound, use the Sound Mixer in the LPS Multimedia menu to turn up the microphone or ensure the correct microphone is enabled if multiple microphones are present.

4.11 Using Adobe Reader to Sign Forms

Adobe Reader replaces eVince as the PDF reader in LPS-Public Deluxe distributions. Both programs can read PDF files, but the Adobe Reader program also supports signing PDF forms using digital signatures. The following procedure should be followed to sign forms:

1. Launch Adobe Reader from the Start menu.
2. Open a PDF file containing a signature field.
3. Click on a field with a red flag that says “Sign Here.” This is a digital signature-enabled field.
4. The Add Digital ID dialog displays. Select “My existing digital ID from” and “A file” then click Next.

5. Another Add Digital ID dialog displays. Select “Add digital ID from a cryptographic token” then click Next.
6. Another Add Digital ID dialog displays. The smart card should be present in the “Token Name:” drop-down list. If not, select it. Enter your smart card PIN in the “Password:” field and click Next.
7. Select the correct digital ID for signing the document.
8. Click the SIGN button. The digital signature should be saved into the PDF document.

4.12 Using SharePoint

Using LPS to interact with Microsoft SharePoint collaboration software is a relatively simple process but may vary slightly from methods used in Windows and Internet Explorer, due to the reduced level of integration with Linux and/or Firefox provided by Microsoft. In general, methods are available in LPS to perform the same tasks but the workflow can be slightly different.

Under Windows and Internet Explorer (we’ll just call this “Windows” from here on), you have three options for editing files stored in SharePoint:

1. You can *check out* the file to your local drafts folder. Upon saving and closing the file, you are offered the opportunity to check the file back into SharePoint, thereby updating it on the server.
2. You can click on the filename and open the file directly from the server. This allows you to actively edit the copy stored on the server. Using this method, the file on the server is updated automatically each time you save it within the editing application.
3. You can manually download the file to your local computer, perform edits as desired, save the file, then manually upload the file back to the server using the SharePoint *upload* button.

The third option is essentially how file edits are performed on SharePoint when using LPS. The first two methods are not supported on LPS since they require Internet Explorer and Microsoft Office.

Editing SharePoint Documents

To edit a SharePoint in LPS, use one of the following methods:

1. Right-click on the filename, and do a *save as* to your local computer (the *Downloads* folder is the default destination, and is recommended). Open the *Downloads* folder and double-click on the file to launch the appropriate LibreOffice application.
2. Click on the filename. You will be presented with a pop-up dialog box asking if you want to open the file using LibreOffice. Click the *open with…* button and the default application selected. Within the application, do a *File/Save As* to save it to your local computer (the *Home* or default directory is appropriate, as is the *Desktop*). Note that the *Downloads* folder will not be available if file was not saved to the local system first.

The first method is recommended since the file is first saved to the local system for editing, and is easier to understand. However, the second method will also work.

If you are working with a source file in a newer format than LibreOffice supports, you will have to use the *File/Save As* command to save it in older Microsoft Office formats.

Saving Files to SharePoint

If you want to upload a new file to SharePoint, simply use the *Upload* menu bar command within SharePoint. The process is similar under Windows.

If you want to update an existing file to SharePoint, also use the *Upload* menu bar command. Just be sure you are in the same SharePoint directory containing the original file, and that the edited file has the same filename as the original. When you use the *Upload* command, be sure the *Add as a new version to existing file checkbox* is selected. You also will have the option to add any version comments. Note that this will not work if you have changed the file extension (e.g., from .docx to .doc). If the filename is different, you cannot replace the existing file; you must create a new file on the server.

Using the *Check Out* Feature in SharePoint

The *Check Out* feature in SharePoint allows you to retain exclusive edit rights to a file. It marks the file as unavailable for editing by other users, which prevents write conflicts if multiple people are attempting to edit the file simultaneously. This feature is supported within LPS, but it acts differently than in Windows.

In Windows, if you use the *Check Out* drop-down selection for a SharePoint file, you will mark the file as unavailable and then automatically open the file in the appropriate Microsoft Office application. In LPS, if you use the *Check Out* drop-down selection, you will only mark the file as unavailable. The file will neither be saved locally nor opened automatically in an application. You must use one of the methods listed in the **Editing SharePoint Documents** section to save and edit your file.

When you are done editing your file and want to upload it to SharePoint, you use the same methods described in the **Saving Files to SharePoint** section (i.e., using the *Upload* function). However, if you have (a) checked out the file, (b) saved it with the same filename, and (c) uploaded it clicking the Add as new version checkbox, then you will get an option to click a *Check In* button and add version-specific comments. This method will clear the *Check Out* flag, and allow other people to edit the file.

If you check out a file but subsequently upload it under a different filename, you will not clear the *Check Out* flag on the original file in SharePoint. However, you can perform this step manually, by using either the *Check In* or *Discard Checkout* choices in the drop-down box on the original file in SharePoint. Note that the *Check In* choice will not launch a check-in process, as it does in Windows; it will only clear the *Check Out* flag. Remember that if you don't clear the *Check Out* flag when you add the new version, no one else will be able add new versions of this file.

To summarize, the *Check Out* feature is supported in LPS, but it is a more manual process than under Windows. The *Check Out* flag is set independently of the file being uploaded, where in Windows these two operations are performed simultaneously. In LPS, they must be performed sequentially.

4.13 Encrypting Data

Using Encryption Wizard

The standard LPS distribution contains AFRL's Encryption Wizard software. Encryption Wizard is a Java-based file encryption program that can be used to quickly and easily encrypt sensitive (but not classified) files for local storage and before transmission via email. It provides a graphical user interface and uses strong encryption. Note that this feature may be removed in some LPS distributions.

Encryption Wizard can use shared passphrases, PKI certificates, or both to encrypt files. An encryption wizard file has a .wzd extension, and can be attached to an email message. When sending an encrypted file to another user, you can use their public certificate to encrypt it. DoD users can obtain certificates in three ways:

1. Download the public certificates of anyone with whom you will be communicating. You can use *https://www.whitepages.mil/* to download certificates.
    - Authenticate to the site using your CAC.
    - Find the person with which you intend to exchange encrypted emails by searching.
    - Note their email address; you must use this address to send mail.
    - Click on the name link.
    - Click on the link to Download Certificate.
    - Save this certificate to your root drive, or to an external data stick.
2. You can use Outlook within Windows to save public certificates for use later in LPS. In Outlook (connected to a Microsoft Exchange server, not offline), use the following steps:
    - Open Contacts.
    - Search address books (find in global address list) for your recipient.
    - Right-click the recipient, then select Add to Contacts.
    - Click on the Certificates icon in the menu bar.
    - Click on the Export… button to save the certificate file.
    - Cancel creating the contact (no contact is actually saved if you stop at this point).
3. Encryption Wizard can be used to obtain your public key to share with others. Use Tools, Export CAC certificate to create a .cer file. This key can be given to others with whom you will be communicating. You can also ask others to send you their key this way as well.

See the Encryption Wizard User's Guide in the LPS online documentation for more details about using Encryption Wizard.

Using Outlook Web Access

Users wishing to encrypt data in email using Microsoft's Outlook Web Access (OWA) should note that OWA does not support S/MIME properly on Linux platforms or in non-Microsoft

browsers. OWA users cannot sign or encrypt emails, although they can read signed emails. The Secure Email (Thunderbird and DAVmail) solution does support S/MIME, but some users may wish to use external encryption. Encryption Wizard can be used to encrypt message content and transmit it over government email systems. Both the sender and the recipient need to have Encryption Wizard on their systems, and they need to agree on a passphrase for encryption and decryption (or use public keys, as described above).

4.14 Adjusting LPS Security Settings

Several security utilities have been added to allow for a more customized user experience. There is now a *Security* menu item that contains a few utilities. Other utilities can be configured through Firefox.

DNSCrypt and OpenDNS

DNSCrypt is a feature that wraps DNS communications in an SSL wrapper, making them more secure and private. It is used in conjunction with the OpenDNS service, which provides a known reliable DNS service, and does not involve whatever DNS services are pushed to your client through DHCP.

DNSCrypt is disabled by default. To enable it for your session, use the *Security* menu option under the Start menu, then select *Enable DNSCrypt*. You can test that it works by using the *Check for OpenDNS* utility in the same location.

HTTPS Everywhere

HTTPS Everywhere is a Firefox add-on that selects an https: site as an alternative to an http: site whenever it exists. This feature is enabled by default.

To disable HTTPS Everywhere for your session, open Firefox, then use the Tools/Add-ons menu, select the Extensions tab, and configure HTTPS-Everywhere (click the *Disable* button). If turned off, it can be re-enabled via the same interface. Firefox must be restarted whenever an add-on is enabled or disabled.

NoScript

NoScript is a Firefox add-on that disables JavaScript, Java and Flash. This feature is disabled by default since it will render many web sites unusable. However, many security-conscious users do not want these features enabled in their browser.

To enable NoScript for your session, open Firefox, then use the Tools/Add-ons menu, select the Extensions tab, and configure NoScript (click the *Enable* button). If turned on, it can be disabled via the same interface. Firefox must be restarted whenever an add-on is enabled or disabled.

4.15 Create your own bootable LPS USB Flash Stick

The LPS CD should contain a directory called **InstallToUSB**. While booted into Windows (not LPS), connect a new USB flash stick to your computer and note its drive letter. Next, run the *USBInstall* batch file in the InstallToUSB directory. Follow the prompts and it should install LPS on the flash stick.

Caveats for creating your own LPS on USB:

1. Allow the batch file to format the flash stick. This process prepares the flash stick for use as a boot device; otherwise, it may not boot.
2. The installation script requires admin rights. Under Windows XP, you must be logged in as a member of the Administrators group. Under Vista or Windows 7, this means the command line process where you run the LPStoUSB.bat file must have administrator rights. You can do this by:
    a. Logging in as an administrator with User Account Control (UAC) disabled
    b. Logging in as an administrator with UAC on, but run the command line as an administrator. [Start, Programs, Accessories, right-click on Command Prompt, Run as Administrator]
    c. Logging in as a normal user, but run the command line as administrator as in (b).
3. USB devices and ports are rated at different speeds. Faster ones can boot in less than a minute. Slower ones will take longer, but are usually faster than CDs.

Government users should not create bootable flash sticks using their government computers if their organizations have prohibited connecting flash media.

5 Addressing Common User Problems

While conducting operational testing of LPS, several common user questions and issues were noted. This section describes those problems and discusses ways to either troubleshoot the issue or to work with the LPS support team to identify the problem in sufficient detail that developers can attempt to fix the issue in a future release.

5.1 Hangs During Booting

Issue: The CD boots (dots are shown marching across the screen), but the screen hangs before the graphical desktop is shown. The system is unresponsive to any inputs and does not display any information on the screen.

Likely Cause: Either not enough system memory (at least 1 GB RAM) or unsupported video hardware. Older computers are more likely to have the memory problem. New computers are more likely to have the video problem. The video problem means that a device driver needs to be added to a future product release. It is also possible that the CD was not burned correctly.

What to do: Several solutions can be attempted:

- First check if memory requirements are met. Add more memory if the system is deficient, or use a different computer.
- Test the CD on another computer to see if it boots. If it doesn't, try burning or obtaining a new CD.
- If a video problem is suspected, record the type of computer (manufacturer and model) and type of video hardware (boot into your normal operating system and check via system information displays – exact steps depend on operating system type and version). Send this information to the contacts listed in Section 7.4.

5.2 Can't Connect via WiFi

Issue: System booted, but WiFi cannot be used. Not that individual access points cannot be accessed, but that the system doesn't even present a list of WiFi networks or allow them to be configured.

Likely Cause: If the Network Manager cannot see WiFi hardware (left-click on the Network Manager icon in the bottom right corner; if it does not list 'Wireless Networks' as a header then no WiFi hardware was detected), then LPS does not contain a driver for the hardware.

What to do: Record the type of computer (manufacturer and model) and type of WiFi hardware (boot into your normal operating system and check via system information displays – exact steps depend on operating system type and version). Send this information to the contacts listed in Section 7.4.

5.3 Can't Access PKI web sites

Issue: Firefox can browse Internet web sites but cannot access PKI-enabled web sites that require a CAC. The site can be reached but the user cannot authenticate, often returning a web server error.

Likely Cause: Typically, the problem is the CAC reader hardware does not support the current CCID standard, the user selected the wrong PKI certificate to use on the web site, or the user does not have a valid account on the server.

What to do: Obviously check that a valid Internet connection exists and that the web server is reachable. Then try the following steps:

- Validate that the correct PKI certificate was selected from the CAC. Confusingly, many web sites require the Email Signature Certificate to authenticate – try this one first, unless you know that another certificate type is required.
- Check the firmware revision level of your CAC reader. If you are using an SCM Microsystems CAC reader, note that LPS includes a firmware update utility. See Section 6.6 for more detail. Update the firmware to the latest version.
- Check to see if the CAC reader is connected to a USB3 port (often labeled with an "SS" next to the USB icon. Try a USB2 port instead.
- If you have multiple CAC readers, try unplugging extra ones. Bootable Media does not always recognize multiple CAC readers, or select the correct one.
- If you still cannot connect, contact the help desk for the target web site to make sure your account has not been disabled.

5.4 Need to Sign or Encrypt Email Messages

Issue: Users of Outlook Web Access (OWA) within Firefox cannot sign, encrypt, or decrypt messages. Signed messages can be read, but users cannot sign new messages. Messages cannot be encrypted or decrypted.

Likely Cause: This is a known limitation due to Microsoft's proprietary implementation of an S/MIME control within OWA that doesn't work with non-Microsoft browsers or operating systems.

What to do: Try using the Secure Email (Thunderbird and DAVmail) solution.

As an alternative workaround for encrypting and decrypting messages, use the built-in Encryption Wizard tool. This product can encrypt and decrypt files that can be attached to an unencrypted message. Encryption Wizard runs on multiple platforms and is freely distributable. Note that the sender and recipient must agree to use this approach and share the password or keys used to encrypt the files.

5.5 Need to work with Lotus Forms (XFDL files)

Issue: Users cannot open or edit XFDL files, typically used with Lotus Forms.

Likely Cause: This is a known problem. Lotus Forms does not run under Linux, and the vendor has been unresponsive when approached about creating a Linux-based version.

What to do: An open source XFDL editor is under development, but will take some time to implement. A better solution is to use Adobe Reader and PDF files. Adobe Reader is free and can use smart cards to sign PDF files, which are usable on multiple platforms. If XFDL files must be used, then one approach is to implement a remote desktop solution (such as Citrix) where the XFDL capability is run on a remote PC that is accessed by LPS.

5.6 Not Working with Multiple Monitors or Docking Station

Issue: When using an external monitor as a primary display, LPS might not select the correct screen to use. Unless using a NVIDIA display adapter, you cannot change the primary screen or configure the computer to use multiple displays. This is often a problem when using a docking station with an external monitor, or a computer with multiple video cards.

Likely Cause: Lack of support for advanced vendor-specific features in the video drivers included within LPS. To save size, LPS tends to use generic drivers that provide the most compatibility for the size of the driver. Proprietary drivers can add more features, but they are often huge – not a good tradeoff for a system that must run in memory.

What to do: Currently, if you want to use multiple monitors or to select an external monitor as your primary monitor, you must use a system with NVIDIA video hardware.

5.7 Problems Using Dell Keyboard with Integrated CAC Reader

Issue: The Dell Smartcard Reader keyboard (model RT7D60) appears to not detect an inserted smart card. The user is not prompted for a smart card PIN when a smart card action is performed.

Likely Cause: This is a known problem with how this keyboard was engineered, and how it presents itself to the operating system. It likely is working correctly, but it isn't obvious at all to the user.

What to do: Initiate a smart card action. Watch the keyboard light. It will blink green at first – wait for it to change to solid orange. Enter your smart card PIN on the keyboard's keypad (not the numbers above the home keys on the keyboard). Press Enter on the keypad. You will **not** see a prompt and the smart card PIN will not be displayed on the screen, but the authentication should succeed.

5.8 Can't use some 4G Wireless Cards

Issue: The system supports 3G broadband wireless networking cards for connectivity but not all 4G cards.

Likely Cause: This is a known problem due to driver support in the current Linux kernel version used in LPS.

What to do: Use a supported 3G card now. Try connecting the wireless card to a device such as a Cradlepoint, and then use a wired connection from that device.

5.9 Sound Garbled in Citrix

Issue: When using Citrix, sound is either very quiet or comes through garbled.

Likely Cause: Unknown. This is an open bug.

What to do: There isn't much to do, except live with the problem. The problem is being actively investigated and a solution is being sought. Several varieties of the Citrix client and server configurations have been tested, but none have worked reliably.

6 Troubleshooting

Check the Frequently Asked Questions (FAQ) in the online documentation and on the LPS web site before requesting help.

If you are using a customized LPS build for your organization, contact your organization's computer support help desk first.

Users with a limited amount of computer skills can still do rudimentary troubleshooting. The following scenarios cover common problems and potential solutions.

6.1 Unable to Boot from CD

Make sure the CD-ROM drive is recognized by the computer. You can verify this by browsing the CD after booting your home operating system.

If you are using a Mac, make sure you are holding down the "c" key while booting the computer. Alternatively, you can hold down the *option* key while booting to be presented with a list of bootable devices—select the CD-ROM drive (it may say that it is a Windows disc). If these methods don't work, boot the Mac normally, then open the System Preferences utility in the Applications folder. Select *Startup Disk*, then choose the CD—it may show up as "Foreign OS on CDROM." Restart the Mac. Changing boot devices requires admin credentials.

If you are using a PC, you need to make sure that your computer's BIOS is configured properly. It needs to be set to boot from the CD-ROM drive before the main hard drive, or the CD should be chosen as the boot option from the one-time boot screen.

Follow these steps to troubleshoot a PC:

- Reboot the computer and enter the hardware setup screen. This usually involves pressing certain key(s) during a specific part of the boot process. The specific keys vary by hardware manufacturer and model. The keys are sometimes displayed on the screen during the boot process, and are often a function key (e.g., F1, F10, F12). If the operating system on the computer's hard drive starts to load, you missed the interval where the key can be pressed. Restart and try again.
- Your computer may have a password-protected hardware setup screen. If so, request that your computer support technicians configure your system for you.
- Once you have accessed the hardware setup screen (which may look similar to the screen shown in Figure 51), configure the boot order so that the computer boots from the CD *before* the main hard drive or select the CD from the one-time boot screen.

Regardless if you are using a Mac or a PC, if you have reached this point and LPS still isn't booting, it is possible that your LPS disc is damaged. Try to boot LPS on a different computer. If that doesn't work, contact your organization's help desk to request a replacement disc, or download the latest image from the SPI web site and burn it to a new CD.

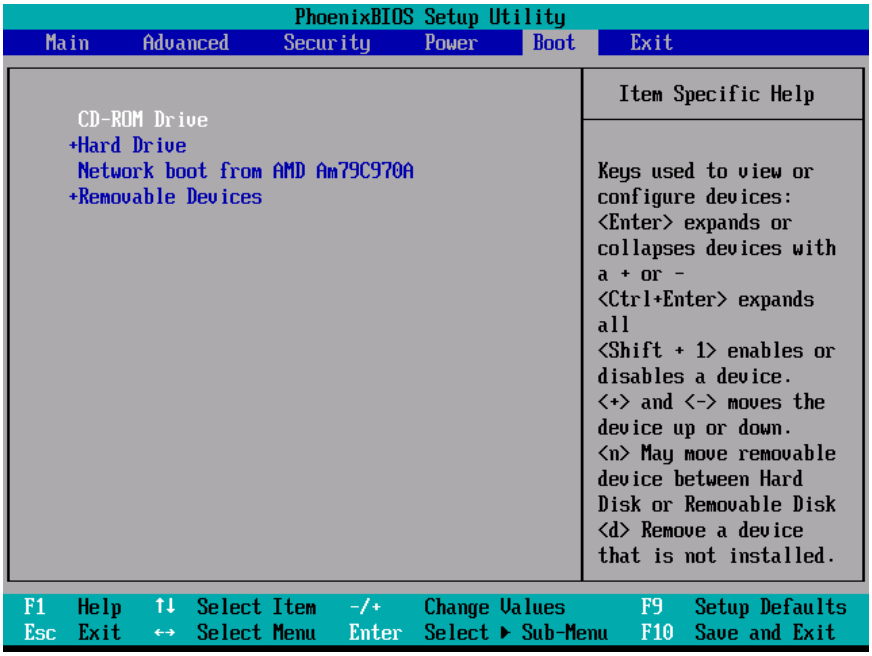

Figure 51 — BIOS Setup Screen

6.2 Unable to Boot from a Flash Memory Stick

First make sure you followed the procedure in Section 4.15 to build a bootable stick. You cannot just copy files to the flash stick.

Next, check that your system allows booting from a USB drive. See the procedures in Section 6.1 to see how to adjust your boot settings. You may have to alter the boot order. You may have to access a one-time boot menu to select the proper settings.

Try inserting the flash stick into a different USB port. Make sure the flash stick works properly by testing it on another computer. Test that the CD used to build the flash stick boots properly; this will test that the image was downloaded and burned properly. If the CD doesn't boot, download the ISO file again and burn it on a new CD (or request a new CD from your help desk), then retry the process.

6.3 Hangs During Booting

If LPS shows the startup screen (dots marching across the screen), the splash screen (graphical screen showing a progress indicator), but then hangs without starting the desktop (the screen with the icons), then the most likely problem is a video driver incompatibility.

First check that your computer meets the system requirements from Section 3.1, particularly the minimum RAM. Assuming that it does, the problem is typically an unsupported video card.

Please contact the LPS help desk (see Section 7.4 for Contacts) with the brand and model of your computer and the type of video card/chip present in your system. We will attempt to find a compatible driver and include it in a future maintenance release.

6.4 Unable to Access the Network

During the LPS boot process, you can observe progress using the startup screen's verbose message display (press F2). A lengthy pause while in the section called Configuring and Starting Network usually indicates failure. Once you reach the LPS Desktop, you can confirm your lack of connectivity by opening the Network Manager and looking for the status indicators as described in Section 4.2.

If you did not receive a warning screen during startup, your computer should have a recognized Ethernet controller with a valid driver. You should still check for connectivity (see Section 4.2) to see if you have a live connection with a valid IP address. If you don't intend to use wired networking, you should use the Network Manager to connect to a wireless or cellular broadband network. If you don't have a recognized wireless controller, please let us know the manufacturer and model so we can add a driver in the future.

If you did not receive a network error message, but you want to use wired networking, then you should start troubleshooting your network connection starting first with the network interface in your computer. Make sure you have a wired network interface in your computer and that it is enabled and working properly. Some computers allow devices to be disabled in the hardware setup. Reboot the system into your home operating system (on your internal hard drive) and test the network connection.

A problem with the network device or the lack of a necessary driver is unlikely to be resolved quickly, and usually represents an unrecoverable error. If there is a physical error with the network device, it will likely have to be replaced. If the network interface is not supported by LPS, then a trouble ticket will have to be opened to log the problem (see Section 7.4 for Contacts).

If the network interface is functioning properly, then you will have to check your network connection and make sure network services are functioning properly. This error exists if your computer does not get a valid network address assigned. This is a much more common error, and usually indicates a basic connectivity problem. Try the following steps to troubleshoot the error:

- Check the physical connection. If using a wired connection, is your computer plugged into the network? Do you know that your cable works properly? Is the network port you are connecting to operational? If using a wireless connection, is your wireless access point functioning properly, and is it connected to the upstream network?
- Make sure you are using a wired, wireless, or cellular broadband connection and not dialup—LPS does not support those connectivity options in this version.
- Be sure you plug in the network *before* you boot into LPS. After you boot LPS, you may have to unplug and reinsert the network cable to get a new address assigned, or use the Network Manager to disconnect and reconnect to a network.
- Check that DHCP services are available and are functioning properly. You know that it works by seeing that an IP address has been assigned. Use the Network Manager to check your IP address, or open an `xterm` command window and type *ifconfig*.

- Boot the computer into your home operating system from your local hard drive. Check that network connectivity works properly. For example, boot your computer into Windows and check network connectivity using Windows-based applications and tools.
- Make sure the DHCP service is available and assigning addresses. This is best tested using your home operating system.

6.5 Unable to Access Local Drives

The internal hard drive of the computer will never be accessible—this is by design. No drivers are present for using the internal hard drive. By default, LPS-Public supports USB-connected devices (hard drives, flash devices, etc.). However, some custom distributions might remove this capability. If you are running a custom distribution, check that USB device support is present. LPS displays a system tray icon for each mounted volume (see Figure 39).

Unplug and reinsert the external device. Make sure it is powered on (if it uses external power). Most USB devices are powered directly by the computer. Depending on the device, there may be a status light that shows that power is being received and that the device is communicating with the computer. Try plugging it into a different USB port, or using a different cable.

Check how the external device is formatted. LPS works with FAT, FAT32 and NTFS formatted volumes.

By default, LPS does not mount the boot device after the booting process is complete. If you booted from a USB flash drive, use a different memory stick as a storage device.

6.6 Unable to use a Smart Card

To troubleshoot this problem, make sure there is a smart card reader attached to the computer and that it functions properly. Verify the following:

- LPS uses the `pcsclite` package for CAC reader driver support. The package developer has provided three lists of devices, supported, should work, and unsupported. Check these lists to see if your device is supported or not.
- Try using an external USB-connected smart card reader. Some computers have built-in readers—the drivers for many of these devices are not loaded in LPS.
- Make sure the smart card reader was connected to a USB port of the computer *before* launching Firefox.
- Run the Diagnostics utility and see if a CAC reader is detected.
- Once booted into LPS, open a command window using `xterm` and check that the smart card reader is recognized by the computer. Type *lsusb* and look at the list of devices present. You should see something like "SCM Microsystems, Inc. SCR331 smart card Reader" listed. If you do not see any devices listed, then the hardware is not recognized by LPS.
- Try connecting the smart card reader to another USB port. Verify that the reader works on another computer.
- Check that you are running the most current version of firmware for your smart card reader. Older versions of readers may have outdated firmware; CCID-standard firmware

is required. If you have an SCM Micro smart card reader, a Firmware Update utility is included in LPS. Follow this procedure to update your reader:

- First, ensure that you know the model number of your smart card reader, and that you subsequently select the correct firmware file. **WARNING: Using the wrong file could permanently damage your reader.**
- Run the *SCRx31 Firmware* utility from the *Utilities* menu.
- Read the instruction screen, click the *Continue* button.
- The **FwUpdate** utility opens. Click the *Browse* button.
- Select the bin file based on the type of smart card reader you have (e.g., SCR331_531_V525.bin for a SCR331 device). Click the *OK* button.
- The **Reader** field should show your smart card reader. Compare the **Firmware Ver** field in the **Current Firmware** column against the **New Firmware** column. If the **Current Firmware** version is lower than the **New Firmware** version, click the *Download* button to update your firmware with the new software. Otherwise, click the *Cancel* button to exit.
- The progress bar should show "Downloading…" then "Verifying…" as the progress indicator moves towards completion. Once finished, the status area should display "Download Success." Click the *Close* button to exit the utility.

Reboot LPS and try to use the smart card reader again.

If your computer recognizes the reader, but does not seem to recognize that a smart card is inserted, check the following:

- Check that the smart card is recognized in the smart card reader. Readers will often use LED lights as a status indicator; look for a status change. For example, on the SCM SCR331 a blinking green light indicates normal operation, but a solid green light means the card cannot be read. Try removing and reinserting the card. Try cleaning the card with a soft, damp cloth and drying completely before using. If that doesn't work, then shut down the computer, remove and reinsert the reader, reboot, and reinsert the card.
- Check that the card was inserted before accessing a PKI-enabled website. If you forget to insert the card first, insert the card, restart the web browser, and try accessing the website again.

If your smart card reader and smart card are working properly, you still may experience some operational issues while using the system. Be aware of the following conditions:

- When you are prompted for a Master Password while using your smart card, remember that this is your PIN. You do not need another password.
- Make sure you are using the correct certificate. Not all web sites use the same certificate, and some will use the Email Signature certificate for authentication.
- NOTE: If you enter an incorrect PIN for your smart card three times in a row, you may need to have it reset at your organizational smart card PIN reset station.

6.7 Defense Travel System (DTS) Doesn't Work

DTS uses a Java-based signing tool that generally works very well with LPS. However, if DTS updates the signing tool, it might not recognize where LPS stores a necessary cryptographic library. If you login to DTS, you should get an "Enter Certificate Password" dialog—this is the correct result. If you instead get a DBsign Client Configuration screen, the library file cannot be found. Simply select the file `/lib/opensc-pkcs11.so` in the "PKCS #11 Library:" field in the DBsign configuration screen as shown in Figure 52. Confirming this configuration via the Save button takes you to the Enter Certificate Password dialog.

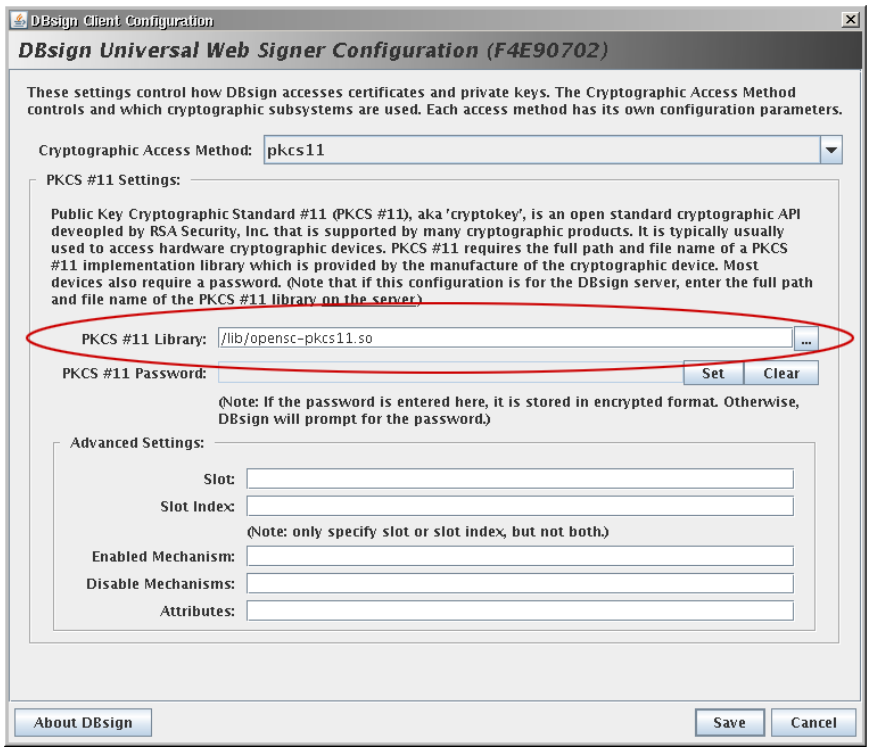

Figure 52 — DBsign Client Configuration Screen

6.8 No Sound

Try adjusting the master volume using the desktop controls. Try opening the Sound Mixer application in the Multimedia menu and adjusting the sound there. Check if sound works through headphones. Check to see if sound is muted in the Sound Mixer application.

Check your specific application to see if there are audio settings. When conferencing, make sure to turn on/up the microphone using the Sound Mixer application in the Multimedia menu. You may also need to adjust settings from within the conferencing application settings menu (such as the Audio Setup Wizard under Manage My Settings in the Meetings menu when using Adobe Connect).

If you still do not hear sound, please let us know what kind of sound hardware is installed on your system. We will investigate and possibly include updated drivers in a future release.

6.9 No Printing

If you cannot print, please check the list of supported printers at http://gimp-print.sourceforge.net/p_Supported_Printers.php. If your printer is not supported, please let us know the vendor and model and we will investigate adding additional drivers in a future release. If the vendor does not supply Linux drivers, it is unlikely we will be able to include support.

Perform basic hardware tests with your printer. If a direct-attached printer, unplug it from your computer and plug it back in. Check the cable connection. If using a USB-connected printer, try moving the cable to another USB port. Make sure the printer is connected to a power source and is powered on. Check the status display of the printer and make sure it is not jammed or otherwise waiting for user action. Check that paper is loaded properly. Make sure the printer works correctly by printing to it from another operating system.

Run the Printer Administration utility (under the Utilities menu). Try to add the printer. See if the printer is detected. Watch for the spinning disk; allow the utility to finish discovering printers.

Try the Help/Troubleshoot option within the Printer Administration utility. See if the printer is listed. If not, select 'Not listed' and then click the *Forward* button. Try searching for a Locally Connected Printer or Network Printer, depending on where your printer is located. If it finds your printer, select it and click the *Forward* button. See if there are any recommended solutions. Close the utility and try to add the printer again; it may be listed under the devices menu now.

If the printer is found and a queue is created, but it still won't print, check the driver. Right-click on the printer queue in the Printer Administration utility, and select *Properties*. Click the *Change* button next to 'Make and Model.' See if the correct driver for the make and model of the printer is selected. If the vendor driver doesn't work, scroll to the top of the list and try the Generic driver (PCL or Postscript, depending on the type of printer).

7 Support

7.1 Warranty

LPS-Public is Government-Off-The-Shelf software, and is supplied as-is with no warranty implied.

7.2 License

LPS-Public uses free software components under the GNU Public License (GPL). The standard LPS software can be freely distributed without restriction.

Some custom distributions may include licensed software products (client access components, etc.). LPS does not confer additional licensing terms beyond those of the underlying products. In all cases, licensed software is included in a distribution for a specific organization. That organization is responsible for managing client access licenses, enterprise agreements, or other licensing vehicles, and for ensuring that all users receiving a custom LPS distribution are properly licensed for any third-party software included.

You are only granted a license to use the software after you have agreed to the following: You will indemnify and hold harmless the author, owner and distributor of the LPS against any and all liability, claims, suits, losses, costs and legal fees caused by, arising out of, or resulting from any negligent, reckless or willful act by you, or from any omission or failure to act by you. You will indemnify and hold harmless the author, owner and distributor of the LPS against any and all liability, claims, suits, losses, costs and legal fees caused by, arising out of, or resulting from any negligent, reckless or willful act by anyone accessing the LPS distribution through you, or any omission or failure to act by anyone accessing the LPS distribution through you. You will make any further distribution of the LPS, if permissible, contingent upon the distributee agreeing to all license terms and conditions.

Please see the software distribution for other possible license terms.

7.3 Copyrights

Adobe® Flash® Player. Copyright © 1996-2010. Adobe Systems Incorporated. All Rights Reserved. Adobe and Flash are either trademarks or registered trademarks in the United States and/or other countries.

Adobe® Reader® Software. Copyright © 1996-2010. Adobe Systems Incorporated. All Rights Reserved. Adobe and Reader are either trademarks or registered trademarks in the United States and/or other countries.

Oracle® and Java™ are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

7.4 Contacts

If issued a custom build of LPS by your organization, contact your normal first-line computer support for problems using LPS. These support teams will have escalation contacts for second-level support. Home users may contact the AFRL directly; support is on a best effort basis. Always check the user instructions, troubleshooting information, and FAQs in this document first.

AFRL provides third-level support and custom development, and handles feature requests (such as supporting additional hardware devices or adding custom applications).

Developer
Air Force Research Laboratory
http://spi.dod.mil
ATSPI_Outreach@wpafb.af.mil