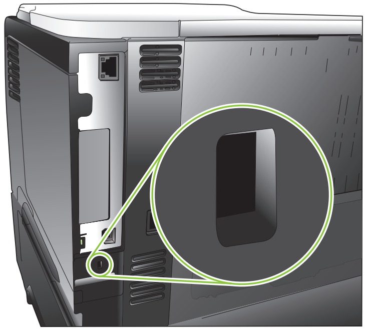
HP LaserJet P3010 Series – Security/Authentication

Security features

How do I?	Steps to perform
Secure the embedded Web server	Assign a password for the embedded Web server to prevent unauthorized users from changing the product settings. 1 Open the embedded Web server by typing the product IP address in a browser address line. 2 Click the **Settings** tab. 3 On the left side of the window, click the **Security** menu. 4 In the **Device Security Settings** area, click the **Configure** button. 5 In the **Device Password** area, type the password next to **New Password**, and type it again next to **Verify Password**. 6 Click the **Apply** button at the bottom of the window. Make note of the password and store it in a safe place.
HP Encrypted High Performance hard disks	This product supports an optional encrypted hard disk that you can install in the EIO accessory slot. This hard disk provides hardware-based encryption so you can securely store sensitive data without impacting product performance. This hard disk uses the latest Advanced Encryption Standard (AES) and has versatile time-saving features and robust functionality.

HP LaserJet P3010 Series – Security/Authentication

How do I?	Steps to perform
Hardware integration pocket	The product has a hardware integration pocket in which you can install a third-party security device. The pocket is on top of the product, behind the control panel. You can connect the third-party device to the product by using one of the internal USB ports. **NOTE**: The hardware integration pocket is not included with the base model.
Secure stored jobs	You can protect jobs that are stored on the product by assigning a PIN to them. Anyone who tries to print these protected jobs must first enter the PIN at the product control panel.
Lock the formatter	The formatter area, on the back of the product, has a slot that you can use to attach a security cable. Locking the formatter prevents someone from removing valuable components from it. 

HP LaserJet P3010 Series – Security/Authentication

How do I?	Steps to perform	
Lock the control-panel menus You can lock various menus on the control panel by using the embedded Web server.	1 Open the embedded Web server by entering the product IP address into the address line of a Web browser. 2 Click the **Settings** tab, and then click the **Security** link. 3 In the **Device Security Settings** area, click the **Configure** button. 4 In the **Control Panel Access Lock** area, select the level of security that you want. 5 Click the **Apply** button at the bottom of the window.	**Minimum Menu Lock** ● The **RETRIEVE JOB** menu requires a PIN for access. ● The **SYSTEM SETUP** menu is locked. ● The **I/O** menu is locked. ● The **RESETS** menu is locked. **Moderate Menu Lock** ● The **RETRIEVE JOB** menu requires a PIN for access. ● The **CONFIGURE DEVICE** menu is locked (all submenus). ● The **DIAGNOSTICS** menu is locked. **Intermediate Menu Lock** ● The **RETRIEVE JOB** menu requires a PIN for access. ● The **PAPER HANDLING** menu is locked. ● The **CONFIGURE DEVICE** menu is locked (all submenus). ● The **DIAGNOSTICS** menu is locked. **Maximum Menu Lock** ● The **RETRIEVE JOB** menu requires a PIN for access. ● The **INFORMATION** menu is locked. ● The **PAPER HANDLING** menu is locked. ● The **CONFIGURE DEVICE** menu is locked (all submenus). ● The **DIAGNOSTICS** menu is locked.

HP LaserJet P3010 Series – Security/Authentication

How do I?	Steps to perform
Secure Disk Erase	To protect deleted data on the product hard drive from unauthorized access, use the Secure Disk Erase feature in the HP Web Jetadmin software. This feature can securely erase print jobs from the hard drive. Data affected (covered) by the Secure Disk Erase feature includes temporary files that are created during the print process, stored jobs, proof and hold jobs, disk-based fonts, disk-based macros (forms), address books, and HP and third-party applications. **NOTE:** Stored jobs will be securely overwritten only when they have been deleted through the **RETRIEVE JOB** menu on the product after the appropriate erase mode has been set. This feature will not impact data that is stored on flash-based product non-volatile RAM (NVRAM) that is used to store default settings, page counts, and similar data. This feature does not affect data that is stored on a system RAM disk (if one is used). This feature does not impact data that is stored on the flash-based system boot RAM. Changing the Secure Disk Erase mode does not overwrite previous data on the disk, nor does it immediately perform a full-disk sanitization. Changing the Secure Disk Erase mode changes how the product cleans up temporary data for jobs after the erase mode has been changed. ● **Non-Secure Fast Erase**. This is a simple file-table erase function. Access to the file is removed, but actual data is retained on the disk until it is overwritten by subsequent data-storage operations. This is the fastest mode. Non-Secure Fast Erase is the default erase mode. ● **Secure Fast Erase**. Access to the file is removed, and the data is overwritten with a fixed identical character pattern. This is slower than Non-Secure Fast Erase, but all data is overwritten. Secure Fast Erase meets the U.S. Department of Defense 5220-22.M requirements for the clearing of disk media. ● **Secure Sanitizing Erase**. This level is similar to the Secure Fast Erase mode. In addition, data is repetitively overwritten by using an algorithm that prevents any residual data persistence. This mode will impact performance. Secure Sanitizing Erase meets the U.S. Department of Defense 5220-22.M requirements for the sanitization of disk media.