HP Color LaserJet CP3525 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 Click the **Device Security Settings** button. 5 In the **Device Password** area, type the password next to **New Password**, and type it again next to **Verify Password**. 6 Click **Apply**. Make note of the password and store it in a safe place.
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. Secure Disk Erase offers the following levels of disk security: • 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.

How do I?	Steps to perform
Secure Disk Erase (continued)	• 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.
Data affected	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.
Job storage	To securely print a private job, use the personal job feature. The job can only be printed when the correct PIN is entered at the control panel.

HP Color LaserJet CP3525 Series – Security / Authentication

How do I?	Steps to perform
Lock the control-panel menus	To prevent unauthorized users from changing the product configuration settings, you can lock the control-panel menus. You can use HP Web Jetadmin to simultaneously lock the control-panel menus on several products. 1 Open the HP Web Jetadmin program. 2 Open the **DEVICE MANAGEMENT** folder in the drop-down list in the **Navigation** panel. Navigate to the **DEVICE LISTS** folder. 3 Select the product. 4 In the **Device Tools** drop-down list, select **Configure**. 5 Select **Security** from the **Configuration Categories** list. 6 Type a **Device Password**. 7 In the **Control Panel Access** section, select **Maximum Lock**. This prevents unauthorized users from gaining access to configuration settings.

HP Color LaserJet CP3525 Series – Security / Authentication

How do I?	Steps to perform
Lock the formatter cage	The formatter cage, on the back of the product, has a slot that you can use to attach a security cable. Locking the formatter cage prevents someone from removing valuable components from the formatter.