



white paper

HP Print Server
Appliance 4250

July 2003

Understanding Authentication and Authorization with the HP Print Server Appliance

(Web Jetadmin version 7.2 and above; PSA Firmware version 2.4.x and above)

Overview

With earlier firmware versions of the HP Print Server Appliance (PSA), administrators were required to maintain a separate user name and password for the PSA's web interface. This meant that the administrator had to maintain duplicate information for the PSA and for their NT Domain user database.

For the PSA, administrators only have to maintain one user name and password that can be used for both the PSA and for the NT account.

Description of the HP Print Server Appliance 4250

The PSA is a network device used to manage and monitor printing over a network (Figure 1). It has been designed to provide a quick and easy way to add print capacity and off-load print spooling and services from the general-purpose servers.

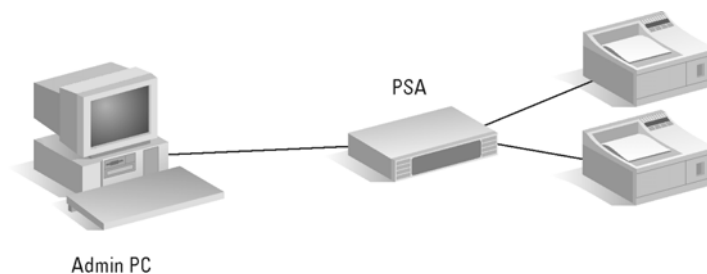


Figure 1 – A Print Environment with an HP Print Server Appliance 4250

Authentication and Authorization with the PSA

When you first connect to an unconfigured PSA, a prompt is displayed requesting your user name and password. The default values are "admin" for the user name and "admin" for the password. (These should be changed.) This standard protocol offers basic authentication to web users.

Secure Sockets Layer (SSL) connections encrypt data including the user name and password, while normal HTTP connections offer no encryption for the user name and password. To be sure all connections use SSL select Encrypt all web communication on the **SSL Settings** page (in the PSA's

web interface under **Security→SSL Certificate**), or, to specify SSL use for a single browsing session the URL should be as follows:

https://ip_address

There are two types of administrator accounts on a PSA:

- Local Administrator Accounts - exists only on a specific PSA. The PSA is shipped with one default Local Administrator Account called "admin".
- Microsoft Domain Accounts – exists in your Microsoft Domain. In order for a domain account to be used, the PSA must first "join" the domain. Once joined, administrators can use their existing users and groups to provide authentication to a PSA.

Not all interactions between an administrator's PC and the PSA occur over the standard web protocol (http). Some of the interactions use the Microsoft Networking Protocol (SMB). These interactions occur when an administrator adds a new driver to the PSA. To install the driver, a small Win32 program is installed from the PSA's web interface. This Win32 program runs as the user logs onto the local PC, which can use different credentials than the user name and password used to log onto the PSA's web interface. In this scenario, the user name and password that the administrator uses on their PC must have a corresponding Local Administrator Account on the PSA with administrator privileges in order to install software, drivers, and printers. For example, if the administrator is logged on to the PC as "charlie" with a password of "snoopy", there must also be a Local Administrator Account on the PSA with the user name "charlie" and the password "snoopy" and administrative privileges.

Microsoft domain security offers an alternative to maintaining duplicate accounts and passwords. This feature also allows you to use Microsoft groups in order to manage access. Single Sign On offers an additional level of convenience, bypassing the PSA's web interface login prompt for users of Microsoft's Internet Explorer (IE). To use this feature, configure IE to bypass the proxy for the PSA and to regard the PSA as part of the "Intranet Zone". Then, the next time you access the PSA's web interface, the authentication will occur in the background using a more secure password encryption than used for basic authentication. Your user still needs administrative privileges on the local PC, but you will no longer need to maintain duplicate passwords.

Security Between Browsers and Web Jetadmin

Web Jetadmin 7.2 includes the ability to manage access to its web interface using a tool called Profiles. A profile requires Web Jetadmin users to type a user name and password. Profiles can integrate with existing Microsoft Windows Domain users if the Web Jetadmin server is a member of a domain.

Security Between Web Jetadmin and the PSA

When accessing a PSA, Web Jetadmin authenticates users with the same protocols, accounts, and procedures as a web browser would use. Most of the traffic between Web Jetadmin and a PSA occurs over http using HTTPS (Secure Sockets Layer (HTTP using SSL for data security) so that the user name and password are encrypted. Web Jetadmin offers several ways to determine which account to use on the PSA; all require the PSA to be configured to allow that user name and password.

The user name and password can be a Local Administrator Account on the PSA, a domain user with administrator privileges, or a member of a domain group assigned administrator privileges.

Some important points to remember are:

- If you configured WJA to require a domain login in order to access Web Jetadmin, Web Jetadmin will re-use those credentials when accessing a PSA.
- A user name and password can be stored for each PSA in Web Jetadmin under:
General Settings → Current Profile → Settings → PSA Security.

A Simple Configuration for a Single Administrator

Many operations have just one administrator using Web Jetadmin to manage the print infrastructure (Figure 2). This configuration is easier to configure while still offering full control over the print infrastructure. A Local Administrator Account is created on the PSA and then associated with the Admin profile in Web Jetadmin. After this is done, Web Jetadmin uses that account for all of its activities on the PSA.

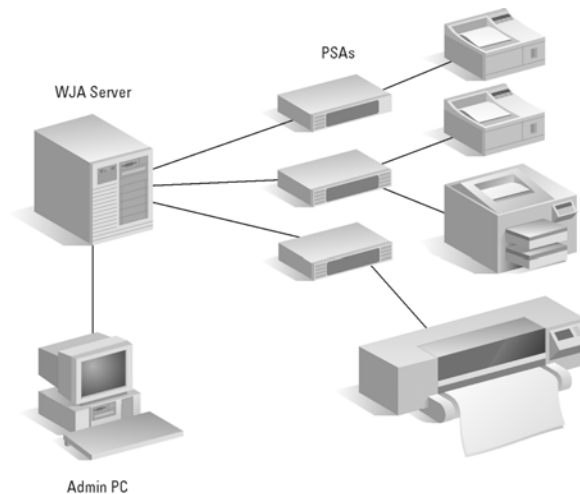


Figure 2 – One Administrator Using Web Jetadmin to Manage Multiple PSAs

A local administrator account can be created on the PSA through the **Administrators** page in its web interface (Figures 3 and 4):

1. Access your PSA's web interface.
2. Select **Administrators** (Figure 3).
3. Click **Add**. The **New Local Administrator** page is displayed (Figure 4).
4. When adding the administrator, be sure to use the same case everywhere; a local administrator account is case sensitive.

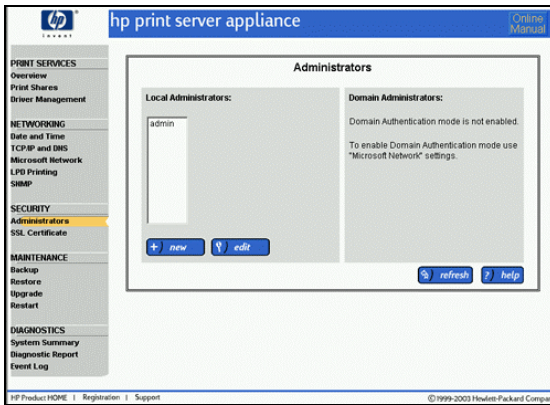


Figure 3 – PSA's Administrators Page

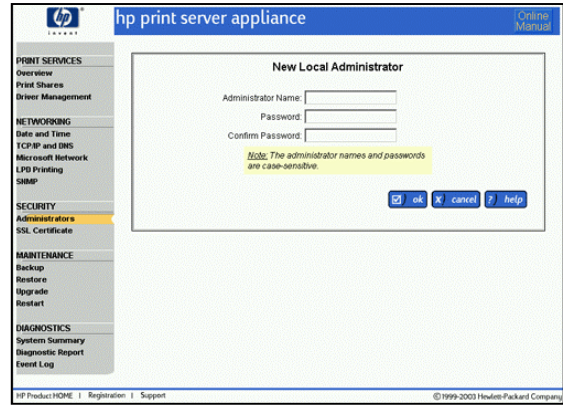


Figure 4 –PSA's New Local Admin Page

This configuration means that whenever Web Jetadmin has to authenticate with a PSA, it uses the Web Jetadmin account. Changes and other events will appear up in the PSA's **Event Log** (in the PSA's web interface) from the user account in Web Jetadmin. One drawback to this configuration is that a second Local Administrator Account is required in order to add drivers and it must have the same user name and password as the account the administrator uses to log into their local system. If these accounts are not synchronized, an error message will appear when the administrator tries to add a driver.

Web Jetadmin uses profiles to maintain identity within its framework. By default, it uses a profile named "Admin". A PSA's local administrator account can be associated with a specific Web Jetadmin profile by accessing Web Jetadmin; use that profile and set the PSA's local account information:

1. Access Web Jetadmin by typing its IP address in your browser.
2. Access **General Settings -> Current Profile Settings (Admin) -> PSA Security**.
3. On the **PSA Individual Authentication** page, highlight the PSA (Figure 5).

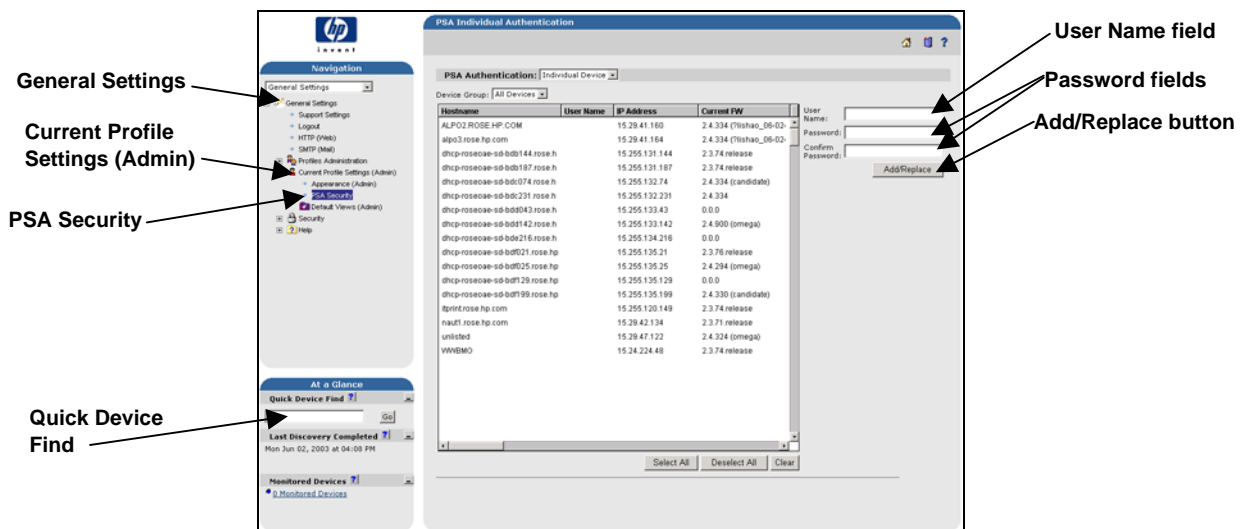


Figure 5 – PSA Individual Authentication (in Web Jetadmin)

4. Type the user name in **User Name** and its password in **Password** and click **Add/Replace** (see Figure 5 above).
5. For more information about Web Jetadmin profiles, see the whitepaper titled “Profiles in HP Web Jetadmin” (http://www.hp.com/go/wja_whitepapers).

To see this configuration in action, access Web Jetadmin and use Web Jetadmin’s **Quick Device Find** feature to find the PSA within Web Jetadmin:

1. Access Web Jetadmin.
2. In the **Quick Device Find** field (see Figure 5), type the name of the PSA and click **Go**.
3. At the top of the **Device Status** page, select **Driver Management** from the drop-down menu (Figure 6).

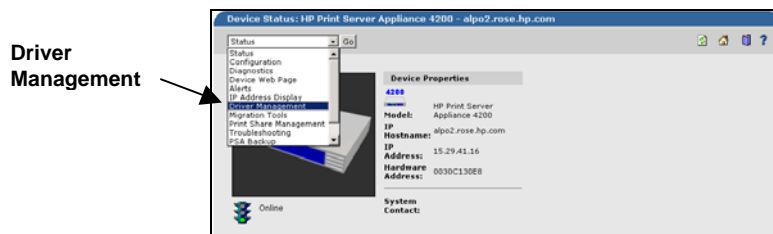


Figure 6 – Device Status PSA Individual Authentication Page (in Web Jetadmin)

4. On the **Printer Driver Management** page, highlight a driver that isn’t being used and click **Remove** (see Figure 7).

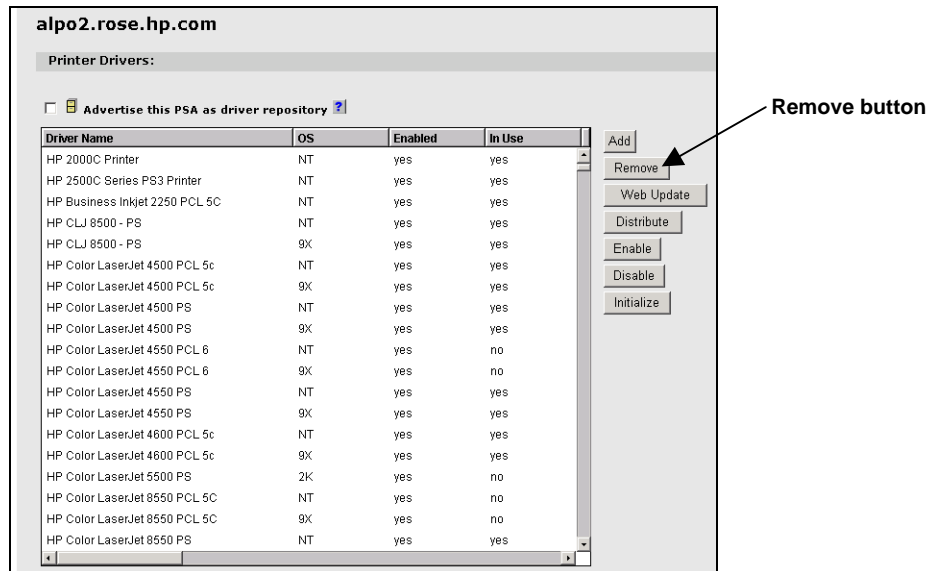


Figure 7 – Select a Driver to Remove on the Printer Driver Management Page

- Return to the PSA's web interface and select **Event Log** (on the menu under **Diagnostics**). Figure 8 shows the message that will be written to the Event Log.

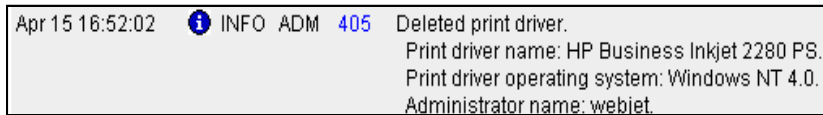


Figure 8 – Entry in the PSA's Event Log

If the administrator name is different from the one you created as a local account and associated with the profile, the configuration change has not worked. For example, you might see an administrator name of "admin", which means that Web Jetadmin used the default name and password (admin and admin) to delete the driver. In this case, make sure you have typed the name and password the same in all locations.

Multiple Administrators with Multiple PSAs

Many environments require multiple administrators to manage their print infrastructure using Web Jetadmin (Figure 9). Using Microsoft's Domain groups allows a flexible configuration that integrates with existing user accounts and allows administrators to be added or removed using Microsoft's user management tools.

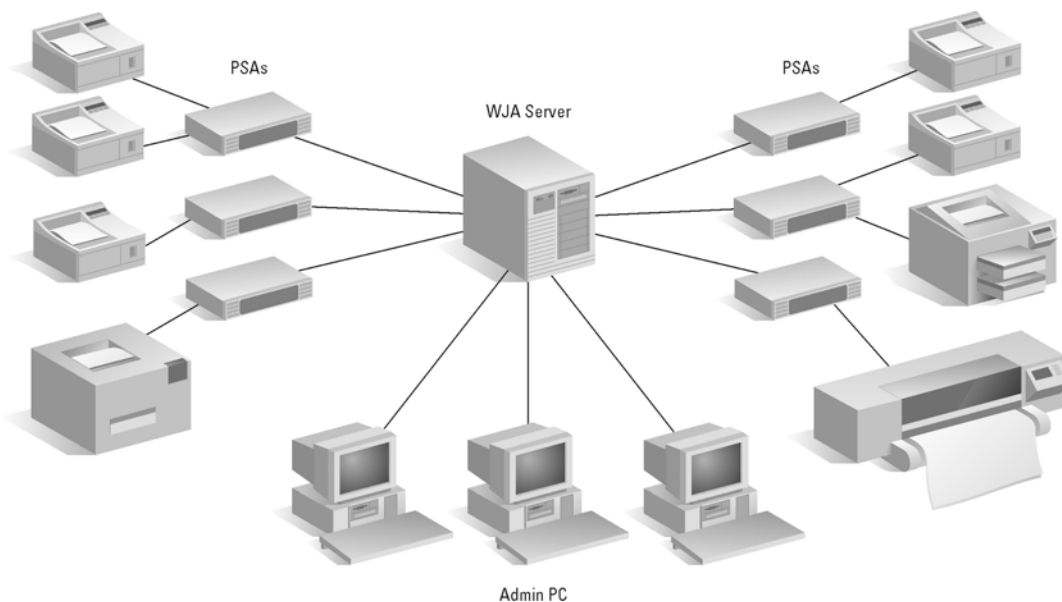


Figure 9 – Multiple Administrators Managing Multiple PSAs

Follow these steps to set up a Microsoft Domain Group with the PSA.

- Create a Microsoft Windows Domain Group for the PSA Administrators: Use the standard Microsoft Tools to creating the group. For Windows 2000, the tool is **Active Directory Users and Groups** (Figure 10).

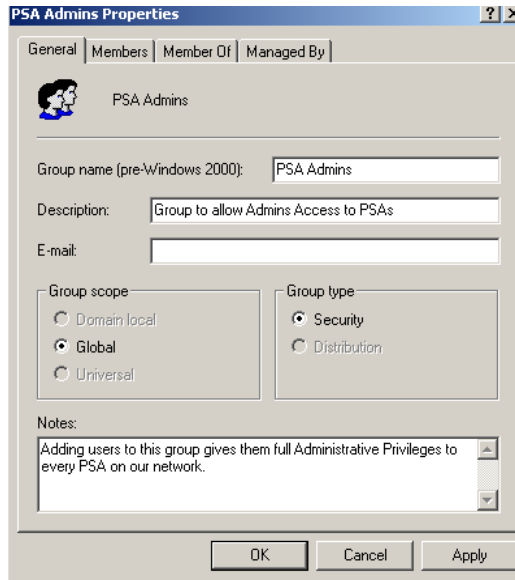


Figure 10 – Active Directory Users and Group Tool for Microsoft Windows 2000

2. Assign the group to the PSAs: After the group has been created and the appropriate users have been added to that group, the group must be added to each PSA as an administrator (Figure 11).

Before adding the group to the PSAs, each PSA must be joined to the domain. See the user documentation on the CD shipped with the PSA for instructions on joining the domain (**Security**→**Administrators**→ **Domain Administrator Accounts**).

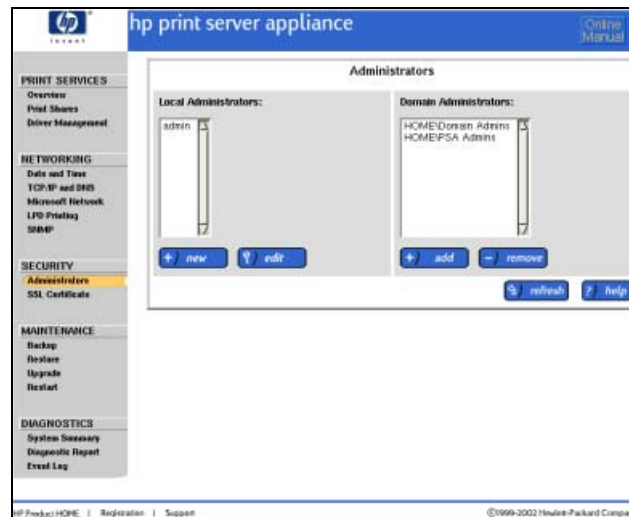


Figure 11 – Administrators Page With Domain Groups

3. Associate the group with a profile in Web Jetadmin:
 - a. The Microsoft windows system running Web Jetadmin must be joined to a domain. It doesn't have to be the same domain as the PSAs, but there must be a trust relationship between the two.
 - b. Assign a password to the Admin profile.
 - c. Change the authentication method to NT Domain/User.
 - d. Add a profile (for example, PSA Admins).
 - e. Select **Authentication**; associate your Microsoft windows group with the profile.

The first time you access Web Jetadmin after configuring it to use NTLM authentication, a login page is displayed (Figure 12). Any user name and password that is a member of the Windows group just added should now be able to log into Web Jetadmin. When that user makes changes to a PSA through Web Jetadmin, the user name and password will be passed through to the PSA.

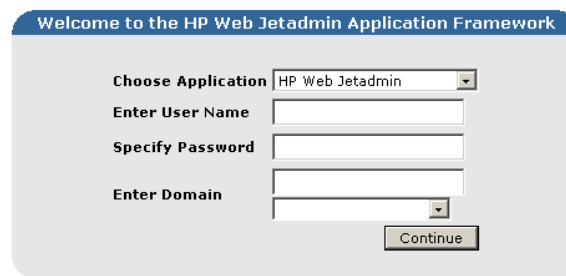


Figure 12 – Web Jetadmin Login Page

4. Assign administrative privileges on the PC: Add the new Windows group to the PSA's Local Administrators group (In the web interface, select **Administrators**→**Add**). This is required before drivers can be added to a PSA.
5. After the environment is configured, you should add a driver to one of your PSAs and push the driver out to all the other PSAs:
 - a. In Web Jetadmin, use the **Quick Device Find** feature to locate one of the PSAs.
 - b. Select **Driver Management** from top drop-down menu.
 - c. Select **Add** and follow the **Add Driver Wizard** instructions to add a driver to the PSA.
 - d. After the driver has been added to that PSA, go back to the **Driver Management** page, highlight the driver and select **Distribute**.
 - e. On the **Driver Distribution** page, select the PSAs just configured for this domain account and distribute the driver.

Sample Authentication Processes

The following two scenarios show the benefits of the authentication process for the PSA:

For a brand new PSA, follow these steps:

1. Purchase and unpack a PSA.
2. Follow the instructions on the Quick Start Guide and in the Rackmount Kit to set up and configure the PSA and add it to the NT Domain (both are shipped with the PSA).

Note: Supported web browsers are Netscape Navigator 6.0 or greater and Microsoft (R) Internet Explorer 5.5 or greater

3. In your web browser, type the PSA's URL or IP address.
4. When the **Security Authorization** page is displayed requesting a user name and password, type the default of "admin" and "admin".
5. Select **Administrators** (on the menu in the web interface under **Security → Administrators**).
6. Select and add accounts for administrators from the list of users and groups.

If administrator accounts have already been configured on the PSA, follow these steps:

1. Using a Microsoft Domain client, start Microsoft's Internet Explorer.
2. In your web browser, type the PSA's URL or IP address.
3. You can now access the PSA without being asked for a user name and password.

Summary

Firmware version 2.4.x for the PSA enables an administrator to use an existing NT Domain user name and password when accessing the PSA. Once they have been authenticated, administrators are not prompted for a password when signing on. Even though the administrator can experience an easier sign-on process, the performance of the PSA is not degraded.

For More Information

<http://www.hp.com/support/printappliance>
http://www.hp.com/go/psa_whitepapers
http://www.hp.com/go/wja_whitepapers