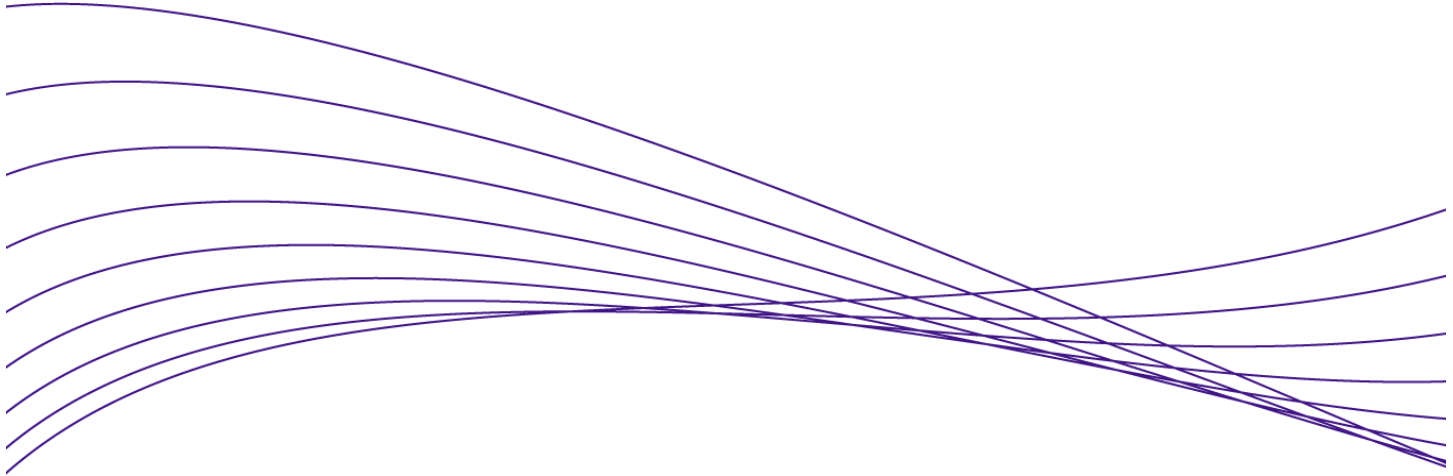


USB Secure Management for ProCurve Switches



Introduction	2
A simple solution with multiple uses.....	2
Staged deployment	2
Remote deployment or upgrade	3
Troubleshooting	3
Physical security	3
Solution architecture	4
IT and business benefits.....	5
Putting the solution to work.....	6

Introduction

ProCurve Networking by HP maintains a design goal to simplify the deployment, use, and management of all of its products—through automation and other strategies—without sacrificing performance, security, and other crucial capabilities. The latest demonstration of ProCurve’s commitment to reducing complexity across the network while also fortifying security and increasing productivity is the ProCurve USB Secure Management solution.

The USB Secure Management solution uses USB storage—a convenient, flexible, and affordable form of storage—combined with security features to simplify the secure deployment, troubleshooting, and remote configuration of ProCurve switches.

Users can store a configuration on the USB storage, then load the configuration on a ProCurve switch by simply inserting the USB storage into the USB port on the switch that will be configured. More importantly, this process occurs in a secure manner, so that users can control where and for whom this solution is enabled.

The USB solution can report information from switches located in both centrally located facilities and remote sites. This ProCurve solution is unique to the networking industry, representing the first time that USB storage has been used in this way to simplify switch deployment and troubleshooting, as well as for remote switch configuration and provisioning.

The ProCurve USB Secure Management solution consists of three parts:

- A device agent built into the ProCurve switch
- A management application integrated with ProCurve Manager Plus (PCM+) 2.3 with Auto Update 1 network management software
- A non-proprietary USB flash drive

Initially, the USB Secure Management solution works with the ProCurve Switch 8212zl core switch, the ProCurve Switch 5400zl and 3500yl Series intelligent edge switches, the ProCurve Switch 6200yl Series, and the ProCurve Switch 2900 Series. It provides an ideal way to take advantage of ProCurve’s free software updates and is part of the ProCurve Lifetime Warranty*, which covers the 8212zl, 5400zl, 3500yl, 6200yl, and 2900 switches.

A simple solution with multiple uses

The ProCurve USB Secure Management solution is well suited for a number of situations and settings, including:

- Organizations with multiple locations
- Enterprise companies and other large organizations
- Smaller organizations that want to perform troubleshooting remotely
- Any purchasers of new ProCurve switches who want a quick way for ProCurve Manager (PCM) to establish baseline configuration

Following is a look at some use case scenarios for the ProCurve USB Secure Management solution.

Staged deployment

As part of a staged or mass deployment strategy, the ProCurve USB Secure Management solution can be used to conveniently upload a qualified software image and a configuration file to a new switch. This can be done without connecting a computer to the serial port of the switch or connecting the switch to a network. The network administrator need only insert the USB storage into the switch and power up the switch.

Once the commands on the USB storage to upgrade the software and load the configuration file have been executed, the USB LED will indicate successful completion.

* For as long as you own the product, with next-business-day advance replacement (available in most countries). The following products and their related family modules have a one-year warranty with extensions available: ProCurve Routing Switch 9300m Series, ProCurve Switch 8100fl Series, ProCurve Access Control Server 745wl, and ProCurve Network Access Controller 800. For details, refer to the ProCurve Software License, Warranty, and Support booklet at www.hp.com/rnd/support/warranty/index.htm

Built-in security features help ensure that the software image is properly authenticated and that the target hardware verifies that the image applies to it. The network administrator can then remove the USB storage and prepare the switch for transport to its destination wiring closet.

Remote deployment or upgrade

ProCurve switches work with the USB Secure Management solution to automatically configure the switches remotely. In this case, the switch is shipped directly to the remote location and the USB storage (or file contents) is sent by the network administrator to an assistant at the remote location.

The assistant simply powers on the device and inserts the USB storage. Once the configuration of the remote switch is complete, the network administrator can connect remotely, and securely manage the device. This can save the network administrator from having to physically travel to where the new switches are located to provision them.

Even someone with little technical knowledge can “reconfigure” a replacement or upgraded switch that is shipped directly to its final site of operation. This is done by copying a configuration file previously saved on the USB device (best done by a skilled network administrator) and initiating the configuration of the replacement or upgraded switch.

Troubleshooting

The breadth of command-line interface (CLI) commands in the switch is available to the network administrator when using USB Secure Management. This means that the diagnostic commands on the switch can be executed by the USB agent and that the results can be recorded on the USB storage without any connectivity to the switch itself. As a result, the USB Secure Management solution expands troubleshooting capabilities to parts of the network that are not accessible by the network management tools.

For example, if connectivity is lost from the central management tools to a switch, it is necessary to troubleshoot directly at the switch. USB Secure Management makes it easy to collect information from the switch that can be analyzed by the organization to quickly resolve the issue.

With the ability to independently collect information on the associated switches, the USB Secure Management solution also provides a convenient way to perform troubleshooting operations and gather relevant information remotely—without physically traveling to the switch, and without the need for either PCM console access or CLI knowledge by the remote assistant.

Physical security

A USB drive with a command file containing the proper credentials can be used to perform sensitive operations that require physical access to the switch. In cases where the network administrator wants to have these operations available, but also wants to limit the specific individuals who can perform these operations, USB Secure Management provides a convenient solution.

For example, the USB Secure Management solution supports the ability to lock and unlock the front-panel push buttons. These buttons allow the switch configuration to be cleared. With the USB Secure Management solution, only authorized people can use these push buttons to clear the configuration, and an audit trail is created that details who performed the action. A command file can be created so that when the USB storage is inserted into the switch, the buttons are enabled. In addition, when the USB storage is removed from the switch, the buttons are disabled automatically.

Solution architecture

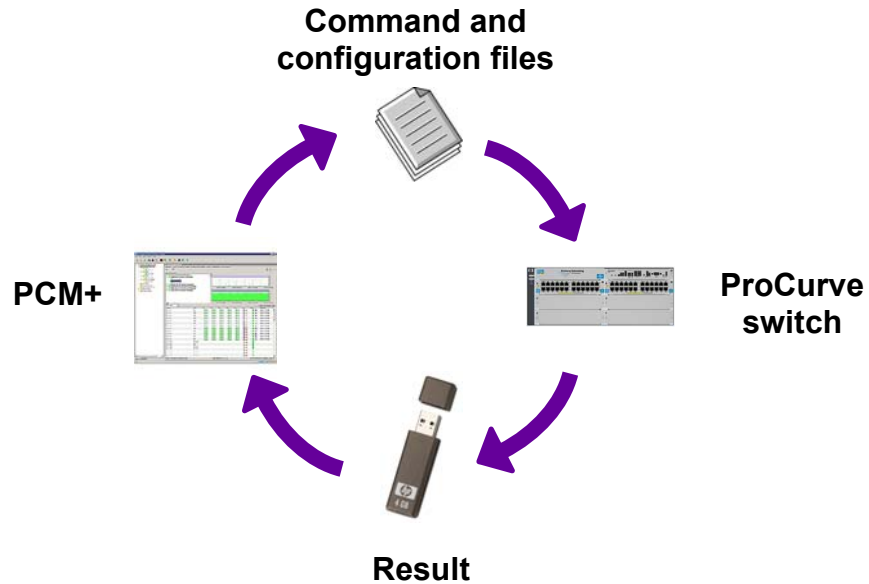
The ProCurve USB Secure Management solution comprises the following components:

- The *USB Secure Management Agent*, a device agent built into a ProCurve switch that securely uses USB storage to load and execute authorized command files and configurations, as well as to store the results of the command file executions. This agent:
 - Executes only command files that have been signed and encrypted by the network administrator
 - Logs the details of command file executions, including the identity of the command file owner
 - Generates a signed report file that gives the details of the command file execution
- The *USB Secure Management Plug-in* to PCM+ 2.3 with Auto Update 1, a management application integrated within the PCM console. This management application:
 - Provides a secure and simple way to create command files
 - Retrieves archived configurations in PCM, to include on the USB storage
 - Verifies the content and structure of the command files
 - Securely writes the commands and configurations on the USB storage
 - Verifies the authenticity of report files on the USB storage
 - Displays the report file contents on the USB storage
- The *Command and Report files*, which are exchanged between the device agent and the management application. The command file:
 - Contains the command sequence to be executed. These commands are expressed as CLI commands.
 - Specifies the device that is to execute the commands. This specification can range from broad (e.g., all 5400 switches should execute this command file) to narrow (e.g., only the 5400 switch with serial number SG0001A01 should execute this command file).
 - Indicates whether this command file should be executed only once by one switch or once each time the USB storage is inserted into the specified switches.

In addition to the ProCurve ProActive Defense security features built into ProCurve switches and available through PCM+ and associated plug-ins, ProCurve has added the following security capabilities to its USB Secure Management solution:

- The USB command files are cryptographically signed by the administrator using PCM+ and verified by the USB Secure Management Agent before execution. As a result, only authorized people can generate these files, and the switch will process only these properly signed files.
- The contents of the USB command files can also be encrypted so that files containing sensitive configuration parameters are protected while they are on USB storage.

- The person for whom a USB command file was created is recorded in that USB command file so that the audit log will contain a record of what was done and by whom.
- The USB result files are cryptographically signed by the switch agent and verified by PCM+ so that an administrator can know that the results reported back by the USB Secure Management Agent have not changed.
- The USB Secure Management solution can be completely disabled, if desired. It can be disabled by default on switches once the switch password is set, and it can be enabled or disabled, as desired, through the CLI.



IT and business benefits

The ProCurve USB Secure Management solution exemplifies ProCurve's overall commitment to making it easier to deploy, manage, and use networking equipment, so that organizations can harness their networks to improve their business performance.

The benefits of this solution from an IT perspective include:

- Less time spent configuring and provisioning switches, especially those located at remote sites
- Faster out-of-the-box configuration and setup of switches
- Greater efficiency by avoiding one-off deployment and support efforts
- Easier troubleshooting of switches
- Greater flexibility in deploying and managing large numbers of switches while maintaining security and control over switch management
- Overall streamlined network operation and greater productivity of IT staff
- Reduced costs of setting up and managing network switches

Broader business benefits of the USB Secure Management solution include:

- **Improved ROI:** ProCurve switches can be up and running quickly, and they can be upgraded and reconfigured without being taken out of service. This contributes directly to increased worker productivity and decreased load on IT staff.
- **Lower personnel costs:** Highly paid technical specialists do not need to spend time traveling to remote locations to configure switches, and many operations can be handled by non-technical staff.
- **Increased flexibility:** Switches can be upgraded and reconfigured quickly to respond to changing business needs.

Putting the solution to work

The ProCurve USB Secure Management Agent will be available with Software Update Release 3 (K13.x for the 8200zl, 5400zl, 3500yl, and 6200yl switches, and T13.x for the 2900 switches). Taking advantage of the complete solution, however, will require the USB Secure Management Plug-in to ProCurve Manager Plus 2.3 with Auto Update 1.

Organizations will then be able to use this innovative solution from ProCurve to streamline their networking operations, deploy and configure network switches securely and more easily, reduce costs while raising IT staff productivity, and protect their investments by utilizing existing hardware in conjunction with a free software update.

With the USB Secure Management solution, ProCurve is once again delivering on its goals of reducing complexity, fortifying security, and increasing productivity—while also lowering the total cost of ownership and boosting ROI.

To find out more about
ProCurve Networking
products and solutions,
visit our Web site at

www.procurve.com



© 2007–2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-6914ENW Rev. 1, February 2008