Sentry Power Manager (SPM) – Software Security

Purpose

This technical note is a detailed review of the security areas of the SPM enterprise software product, version 6.0 and greater, and provides a brief explanation of how the security works.

This document covers security for the access paths and operations of SPM only; security of the data center and physical access to the PDUs are not covered in this document.

Note: For information about the security of Server Technology PDUs (PRO1/PRO2 firmware version 8.0 and later, and CDU1 firmware version 7.0 and later), see the technical note 303-9999-12, PDU Security. Topics include the security of access/hardware communication paths, server protocols, client features, and reset/remote shutdown.

Overview

SPM software security is designed to be proactive, implementing security improvements with every product release. This is accomplished either through security enhancements or through Ubuntu security updates.

Note: If there is an immediate need to address a specific vulnerability, a security patch will be provided and all customers will be notified about the update.

To receive the maximum benefit of SPM software security, Server Technology strongly recommends that you operate with the current SPM version and keep your SPM versions up-to-date. For assistance with upgrades and obtaining the latest SPM version, contact Server Technology Technical Support at: support@servertech.com

SPM's Authentication Method

Users

Access to SPM – via web, file transfer, CLI, or API – is based on secured user accounts and user groups. Capabilities are the predefined levels of user group access to SPM system objects as granted by the SPM administrator (or power user) to individual user groups.

SPM User Types

SPM recognizes the following user types:

User Level	Capability
Administrator	Full access for all configuration, control (On, Off, Reboot), and status. For system security, only the administrator level users can add or modify other user levels.
Power	Same capabilities as the Administrator user account but without user management capabilities.
Regular	Access to view and limited access to configure some objects in the system. Access rights for regular users can be configured per object: No Access, Off, On, Outlet Control, Reboot, Setup, and View Only.

Access Rights in SPM

SPM restricts access based on the three user group levels: Administrator, Power, and Regular (described in the previous table), and the six per-object permissions (described in the following table).

Permissions are the predefined levels of access rights that a user has to specific system objects/resources as granted by the SPM administrator. To ensure system security, it's recommended that SPM users are granted only the minimal permissions necessary to perform their jobs.

Note: Permissions apply only to users who are members of a Regular user group, not members of an Administrative or Power user group.

SPM recognizes the following permissions:

Permission	Description
No Access	User has no access to any of the SPM system objects.
Off	User has partial access for control (Off). Off is available only to SPM system objects that contain outlets.
On	User has partial access for control (On). On is available only to SPM system objects that contain outlets.
Outlet Control	User has full outlet control and view access. Outlet Control is available only to SPM system objects that contain outlets.
Reboot	User has partial access for control (Reboot). Reboot is available only to SPM system objects that contain outlets.
Setup	User has full Administrator access to the PDU.
View Only	User has data view access only. User cannot save changes and user cannot perform actions on SPM system objects.

Changing the Default Password

The default SPM administrative user is the **admn** user account: username/password = admn/admn. The admn user may grant full administrative access level rights to other administrator user groups.

Notes:

- There is no "i" in the admn username or password.
- The admn user account cannot be deleted or demoted but it can be renamed.

For SPM security, it is strongly recommended that you log in and change the username and/or password of the default admin user account.

User Lockouts

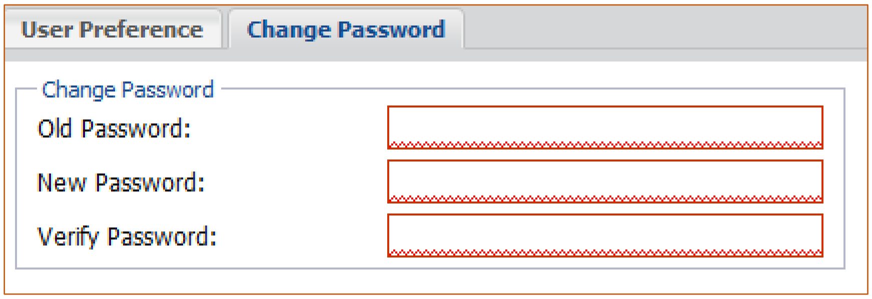
Login Attempts

A lockout occurs in SPM for any five consecutive login attempts. After the fifth invalid login attempt, the user is locked out of SPM for five minutes. After five minutes, the user can then log in again with the valid username/password combination.

If the user forgets their login or password, they should contact their SPM administrator to rest the password. However, if a valid administrator login is not known, the administrator must contact Server Technology Technical Support at support@servertech.com to reset their password.

Password Changes:

Individual users can change their own SPM passwords at My Account > Change Password tab.



Change Password

Old Password:

New Password:

Verify Password:

Four invalid attempts in the Old Password field will log out the user and the SPM Login window will be displayed.

SPM uses this behavior as a security measure in case the user left the browser open while logged in to SPM and someone else tries to take advantage of the situation to change the user's password.

Ubuntu Operating System

Ubuntu Versions

SPM uses Long Term Support (LTS) versions of Ubuntu to ensure that security patches are installed and available for newly discovered vulnerabilities. Ubuntu issues security patches for LTS versions for five years. SPM 6.0 and 6.1 use Ubuntu 12.04 LTS, and SPM 6.2 uses Ubuntu 16.04 LTS.

Ubuntu Security Patches

When Ubuntu publishes a security update for a vulnerability that may compromise the security of SPM, a patch is made available to SPM customers to apply the Ubuntu security update, as well as all other security updates up to that date.

Note that the latest security releases are applied to new versions of SPM via Ubuntu even though the Ubuntu version number may be older. SPM uses Ubuntu's official releases on nearly all available packages. Ubuntu works with SPM developers to ensure security fixes are applied to older versions that are frozen in time by the Ubuntu official release.

For example, the Apache web server version 2.4.18-2ubuntu3.4 has all the features of version 2.4.18, but it also has all the applicable security and bug fixes of later releases of Apache. Many security scanning tools only do a simple version number check and do not test their vulnerabilities.

Ubuntu's CVE tracker can be used to determine if a given vulnerability affects the SPM's version of Ubuntu and package: http://people.canonical.com/~ubuntu-security/cve/

In addition, the changelog of individual packages can be reviewed to determine what security fixes have been backported to it: http://packages.ubuntu.com

SPM has never to-date encountered an issue where Ubuntu does not support their older releases. If the situation ever arises, SPM developers are committed to performing the manual work to upgrade the release.

Important: To promptly receive Ubuntu security updates, Server Technology strongly recommends that SPM customers keep their SPM version up-to-date.

Embedded Components

The following table shows the main tools SPM uses:

Component	Version in SPM 6.1.3	Version in SPM 6.2.2
apache2	2.4.25 custom build	2.4.18-2ubuntu3.5
bash	4.2-2ubuntu2.6	4.3-14ubuntu1.2
cron	3.0pl1-120ubuntu4	3.0pl1-128ubuntu2
linux-image	3.13.0-117.164~precise1	4.4.0-101.124
openssh-server	1:5.9p1-5ubuntu1.10	1:7.2p2-4ubuntu2.2
openssl	1.0.2k custom build	1.0.2g-1ubuntu4.9
php	5.6.30-10 custom build	7.0.22-0ubuntu0.16.04.1
postgresql	9.3.16-1.pgdg12.4+1	9.5.10-0ubuntu0.16.04
rrdtool	1.4.7-1ubuntu1	1.5.5-4
smbclient	2:3.6.25-0ubuntu0.12.04.10	2:4.3.11+dfsg-0ubuntu0.16.04.12
snmp	5.4.3~dfsg-2.4ubuntu1.3	5.7.3+dfsg-1ubuntu4
vsftpd	2.3.5-1ubuntu2	3.0.3-3ubuntu2

Hardening Guidelines

SPM security hardening is based on the CIS Ubuntu Security Benchmarks:

https://www.cisecurity.org/benchmark/ubuntu_linux

In some cases the guidelines are not applicable to SPM, or alternate measures are taken to mitigate the risk. Besides Ubuntu updates, SPM uses continuous security improvements with iterative security updates as the SPM product is expanded and improved.

SPM's Cryptography

Password Encryption

Passwords are transferred with AES-256 encryption.

SSL

SSL is provided through OpenSSL.

SPM 6.0.2 and greater supports versions TLS 1.0, TLS 1.1, and TLS 1.2.

SPM 6.1.2 and greater supports cipher suites ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-SHA, DHE-RSA-CAMELLIA256-SHA, AES256-SHA, CAMELLIA256-SHA, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-SHA, DHE-RSA-CAMELLIA128-SHA, AES128-SHA, and CAMELLIA128-SHA.

Protocol Security

Web

It is recommended to use HTTPS and disable HTTP.

In SPM 6.1.2 and greater, the default SSL certificate is self-signed, SHA256 with RSA (2048 bit). In SPM 6.0.2 and greater, a feature was added to allow administrators to replace the default certificate with their own certificate.

Command Line Interface (CLI)

The SPM CLI is for administrative users only. Access to SPM via console, serial, telnet, and SSH use the same SPM CLI for limited access to certain areas of system setup. The recommendation is to use SSH and disable telnet.

File Transfer

For SPM administrative users only. File transfer allows read/write file access to a limited part of the SPM system, mainly used for upgrades, backups, and restores. The recommendation is to use SFTP and disable FTP.

API

SPM has an API that can be enabled by entering a separate license key. The API provides programmable access to the majority of the GUI functionality and data. Access to the API is permitted for all SPM users. The same user types and user permission levels as web access are also used in the API.

It is strongly recommended to access the API only via HTTPS so that communication is protected with the SSL encryption layer. For better encryption security and to defend against man-in-the-middle attacks, a custom SSL certificate is recommended.

To initiate an API session, the user credentials must be sent to SPM with the password hashed with MD5. No other password hashing options are supported at this time. The remainder of the session is authenticated with a unique random 32-digit session ID that is generated by SPM.

Secure Communication with PDUs

SNMP

It is recommended to use SNMP v3 and both encryption passphrases 8 or more characters for more secure communication between SPM and the PDUs.

SNAP

SPM uses a proprietary protocol called SNAP to send configuration parameters to Server Technology PDUs. The SNAP protocol operates over an HTTPS session. This access method can be disabled or enabled from the PDU.

Logging

SPM logs configuration changes done by users, login attempts, and system events. The more detailed system logs are saved internally and can be exported and sent to Technical Support for troubleshooting. Some system event logs can be accessed by forwarding them to a Syslog server.

Sensitive information, such as passwords, is omitted from the logs.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.

1040 Sandhill Drive Tel: 1-800-835-1515 Web: www.servertech.com
Reno, Nevada 89521 USA Fax: 775-284-2065 Email: support@servertech.com

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.