# Security Enhancements



# Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html

## PSB Requirements for 20.2.0 Release

### Feature Summary and Revision History

***Table 1: Summary Data***

| | |
|---|---|
| Applicable Product(s) or Functional Area | CPS |
| Applicable Platform(s) | Not Applicable |
| Default Setting | Enabled - Always-on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | Not Applicable |

***Table 2: Revision History***

| Revision Details | Release |
|---|---|
| First introduced | 20.2.0 |

### Feature Description

CPS now supports the following PSB requirements:

- Generating SHA-512 algorithm-based hash and salt credentials using OpenSSL.

- Verifying support for current TLS and SSL versions using CAVE tool.
- Verifying harden production software and infrastructure components using cloud9 audit tool.
- Making sure you allow the use of credentials specified in accordance with the credentials CPS offers.
- Deleting unnecessary information (PII).
- Utilizing prepared statements or validating user input to construct XPath queries.
- Disabling entity expansion or validating text content after expansion to prevent XML External Entity (XXE) Injection.

As a part of PSB requirements, the following is added:

- SSH timeout parameter is added. You can define `clientAliveInterval` for OpenStack setup and `client_Alive_Interval` for VMware setup to configure SSH idle timeout. By default, the value is 0 (zero).
- `-f` or `--force` option to the `change_passwd.sh` script to reset the forgotten password only from the root user.
- `generate_encrypt_password.sh` script used to generate encrypted passwords. This method can be used for fresh install and new user. Existing users and passwords will work without any problem. You need to update your old CSV/YAML files with new encrypted passwords.

  When ISSM is performed from an older release to this release, use `generate_encrypted_password.sh` script to generate the encrypted password.

  For more information, see *System Password Encryption* section in the *CPS Installation Guide for VMware*.

# PSB Requirements for UI and API Issues

### Feature Summary and Revision History

***Table 3: Summary Data***

| | |
|---|---|
| Applicable Product(s) or Functional Area | CPS |
| Applicable Platform(s) | Not Applicable |
| Default Setting | Enabled - Always-on |
| Related Changes in This Release | Not Applicable |
| Related Documentation | Not Applicable |

***Table 4: Revision History***

| Revision Details | Release |
|---|---|
| First introduced | 20.2.0 |

### Feature Description

CPS now supports the following PSB requirements:

- CPS UIs are protected against possible server path disclosure risk.
- CPS UIs are protected against Query Pattern in SSL request attack.
- Protects command processors from injecting vulnerabilities by preventing the execution of arbitrary commands or code.
- CPS UIs are protected against SQL injection.
- Policy Builder and Control Center complies with the requirement that the request headers must not contain any sensitive information.