CSP Authenticator+ ™

CSP Authenticator+ is a multi-factor authentication solution for HPE NonStop servers. It supports various authentication methods and can be used as a Safeguard SEEP, or with Pathway (or other) applications.

It provides a RESTful interface to the CSP Authenticator+ web-server in order to support multi-factor logins on HPE NonStop systems.

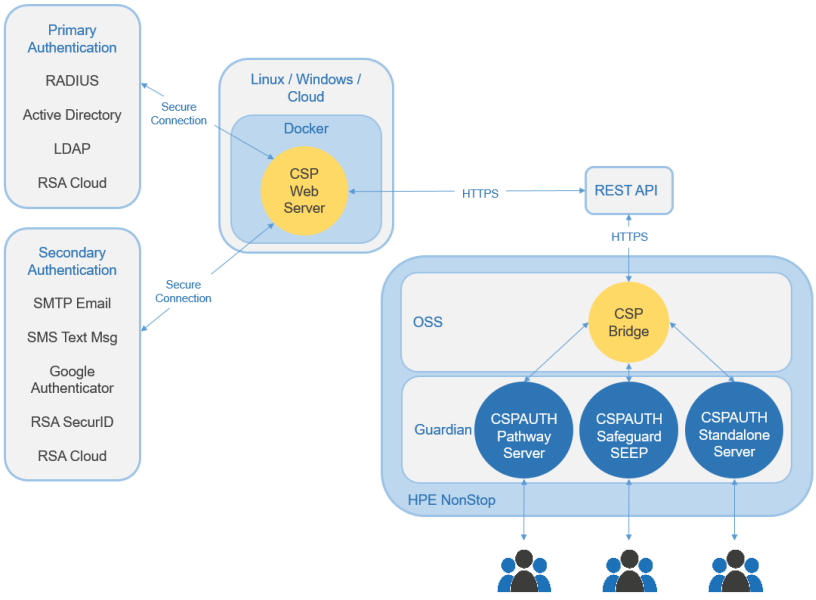
Methods supported include RSA SecurID, RADIUS, Active Directory, LDAP, Email, Text Message, and Google Authenticator. CSP's agile development model allows for inclusion of additional authentication methods, based on specific customer requirements.

What benefits does it provide?

- **Protect valuable resources and data** from attacks
- **Add layers of authentication** for secure access to systems and critical applications
- **Address PCI compliance requirement 8.3**, which requires multi-factor authentication for all personnel with remote access and non-console administrative access to the cardholder data environment
- **Integrate with centralized ID management systems** to effectively manage users

Key features

- Support for multiple authentication methods including RSA, RADIUS, Active Directory, and LDAP
- Provides standardized authentication across platforms
- Configure for all or select users
- Fully encrypted communications with web server
- Support for new authentication methods
- Test mode support
- Self-hosted web application installed on Windows, Linux or Cloud platforms
- Browser based UI with option to disable
- RSA certified
- HPE NonStop Agent supports TACL, Pathway and Non-Pathway applications



Learn more about how enterprise data protection can benefit your organization here or contact us to discuss your data protection requirements: www.comforte.com. Follow us on social media: