# CSP Authenticator +

**Multi-Factor Authentication for NonStop Systems**

## CSP Authenticator +

CSP Authenticator+ provides multi-factor authentication for NonStop servers and supports various authentication methods. It can be used as a Safeguard SEEP or with Pathway and non-Pathway applications. Almost any application, including TACL, can now easily support multi-factor authentication.

The new CSP Authenticator + cloud-native application was developed using a modern cloud-based framework. This redesign focuses on providing security, flexibility, and scalability.

## Safeguard Authentication SEEP

In this mode, all Guardian-user login attempts processed by Safeguard are handled by the Authenticator+ cloud-native application. CSP Authenticator+ may return prompts for RSA token value or issue other challenges such as an Email or SMS OTP, based on a user's configuration.

## Pathway or Non-Pathway Server

In this mode, login attempts through an application, including a Pathway application, are passed to the CSP Authenticator+ cloud-native application for secondary authentication.

## Supports Multiple Authentication Methods

Multiple authentication methods such as RADIUS, Active Directory, RSA, and Open LDAP are supported. Additional authentication methods include Email, Text Message, Microsoft and Google Authenticator.

## Encrypted Communications

All communication with the CSP Authenticator+ cloud-native application is fully encrypted.

RSA READY


## Key features

- Support for multiple authentication factors including RSA, RADIUS, Active Directory, and LDAP, Microsoft, Google, OTP
- Create various profiles and policies for different set of users, and applications
- Ability to use more than two authentication methods
- Provides standardized authentication across platforms
- Configure for all or only selected/privileged users
- Fully encrypted communications with cloud native application
- Supports various databases
- Support for new authentications methods
- Supports TACL, Pathway and Non-Pathway applications

## Benefits

- Protect valuable resources and data
- 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

# CSP Authenticator +

**Multi-Factor Authentication for NonStop Systems**


**CSP Authenticator+ New Cloud Native Application**

## CSP Authenticator+ New Cloud Features

1. New cloud-based framework – A new cloud native application built using modern technologies
2. Support for Kubernetes Helm deployments – easy to deploy in cloud environments using Kubernetes framework
3. Support for High Availability environments – Create highly available Kubernetes clusters for resiliency
4. No differentiation between Primary and Secondary authentication – users can choose any mix of available authentication methods, and even choose more than 2 authentication methods
5. Application based authentication methods are now supported, and more authentication methods are being added. Authentication methods currently supported include RSA, LDAP, Active Directory, RADIUS, Google and Microsoft authenticator, OTP via Email, and OTP via SMS
6. Set different authentication methods for different user groups and privileged groups
7. Redesigned user-interface makes it more intuitive and user friendly
8. Maintain a matrix of authentication profiles, policies (authentication methods), and users
9. Support for various databases, including Amazon S3, Atlas Cloud service, MongoDB, etc.

## CSP - Compliance at your Fingertips™

For more information contact:

***Computer Security Products, Inc.***
Tel: 1-800-565-0415 or 1-905-568-8900
Email us at: Sales-csp@cspsecurity.com
Visit us at: www.cspsecurity.com

Hewlett Packard Enterprise
Technology Partner
SILVER PARTNER