CSP Authenticator +

Multi-Factor Authentication for NonStop Systems

CSP Authenticator+

The new CSP Authenticator+ solution provides a REST interface to the CSP Authenticator+ Web Server in order to support multi-factor logins on NonStop systems. Methods supported include RSA SecurID, RADIUS, Active Directory, LDAP, Email, Text Message and Google Authenticate. CSP's agile development model allows for inclusion of additional authentication methods, based on specific customer requirements.

CSP Authenticator+ can provide authentication services in several ways:

Safeguard Authentication SEEP

In this mode, all login attempts by Guardian users that are normally processed against Safeguard are instead passed to the Authenticator+ agent, which in turn sends the login request to Authenticator+ web server. Based on a user's configuration, CSP Authenticator+ may return prompts for RSA token value or issue other challenges such as an Email or SMS OTP.

Pathway or Non-Pathway Server

In this mode, login attempts through an application, including a Pathway application, are passed to the Authenticator+ agent, which in turn sends the login request to the CSP Authenticator+ web server for secondary authentication.

Primary and Secondary Authentication

In addition to supporting multi-factor (secondary) authentication, CSP Authenticator+ also supports Primary authentication methods such as RADIUS, Active Directory, LDAP & RSA Cloud.

Encrypted Communications

All communications with the CSP Authenticator+ web server are fully encrypted.

RSA® READY

Key features

- Support for multiple authentication factors including SecurID (RSA) tokens
- Support for RADIUS, Active Directory & LDAP
- Use for Primary & Secondary authentication
- Standardized authentication across platforms
- Configure for all or selected users
- Certified for the latest RSA release
- Support for virtual addressing
- NonStop to RSA User Assignment

Configurable

The NonStop agent can be configured to include all or some users and terminals, allowing for the selective use of multi-factor authentication. Additionally, selected NonStop users can be assigned to specific RSA ids.

Test Mode

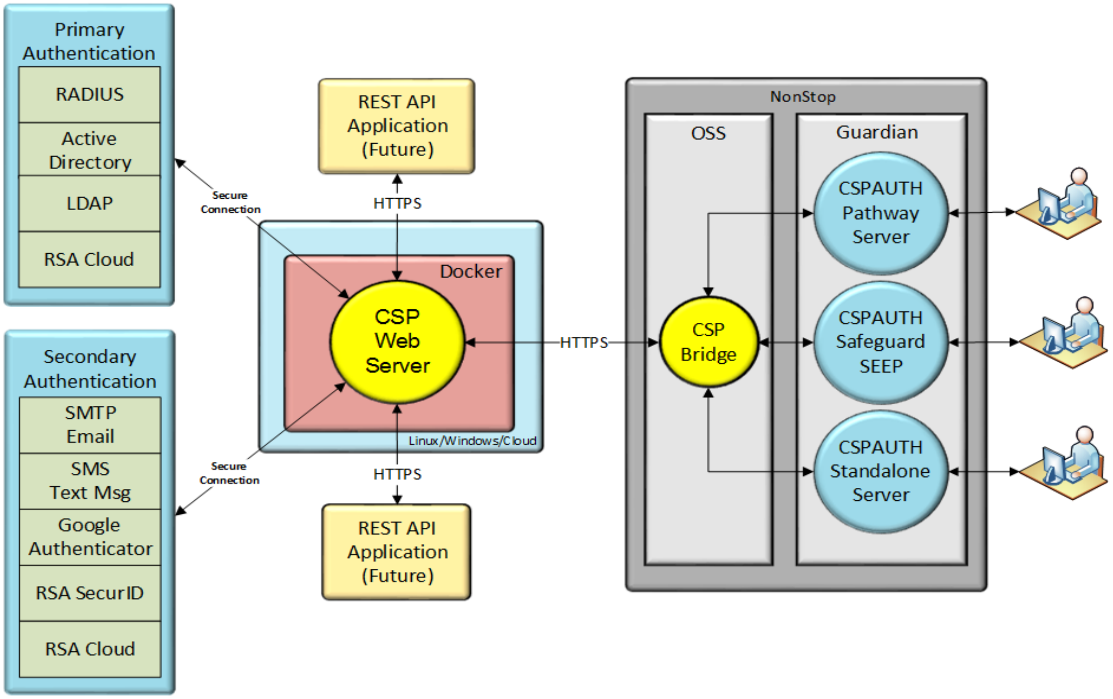
CSP Authenticator+ can also run in "test" mode, allowing the administrator to ensure that:

1. Inclusion/exclusion rules will trigger the appropriate authentication method for each user.
2. The CSP Authenticator+ web server can be reached to authenticate the user based on their system profile.

COMPUTER SECURITY PRODUCTS.INC.

CSP Authenticator +

Multi-Factor Authentication for NonStop Systems



CSP Authenticator+ and the Authenticator+ Web Server

CSP Authenticator+ resides on the NonStop platform and uses an OSS “bridge” to connect via a RESTful interface to the CSP Authenticator+ web server. Almost any application, including TACL, can now easily support multi-factor authentication. Primary authentication methods supported include RADIUS, Active Directory, LDAP & RSA Cloud. Secondary (multi-factor authentication) methods supported include RSA SecurID, RSA Cloud, Email, Text Message and Google Authenticator. User information is securely loaded onto the web server via AES encryption and HTTPS protocols. **No password information is kept on the web server**; only the email address, SMS # or other token serial number associated with the users to whom multi-factor authentication may apply. The administrator is in control of which additional methods (one or many) are to be used and which users and applications must use multi-factor authentication.

The CSP Authenticator+ web server is self-hosted in a secure “sandbox” called a Docker Container, which can be hosted in any UNIX, Windows, MAC or Cloud environment. Each application can have its own Docker container environment if desired.

Hewlett Packard Enterprise
Technology Partner
SILVER PARTNER

Contact Computer Security Products for more information

Tel: 1-800-565-0415 or 1-905-568-8900
Email us at: Sales-csp@cspsecurity.com
Visit us at: www.cspsecurity.com