CSP AUTHENTICATOR +

Multi-Factor Authentication for NonStop Systems

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

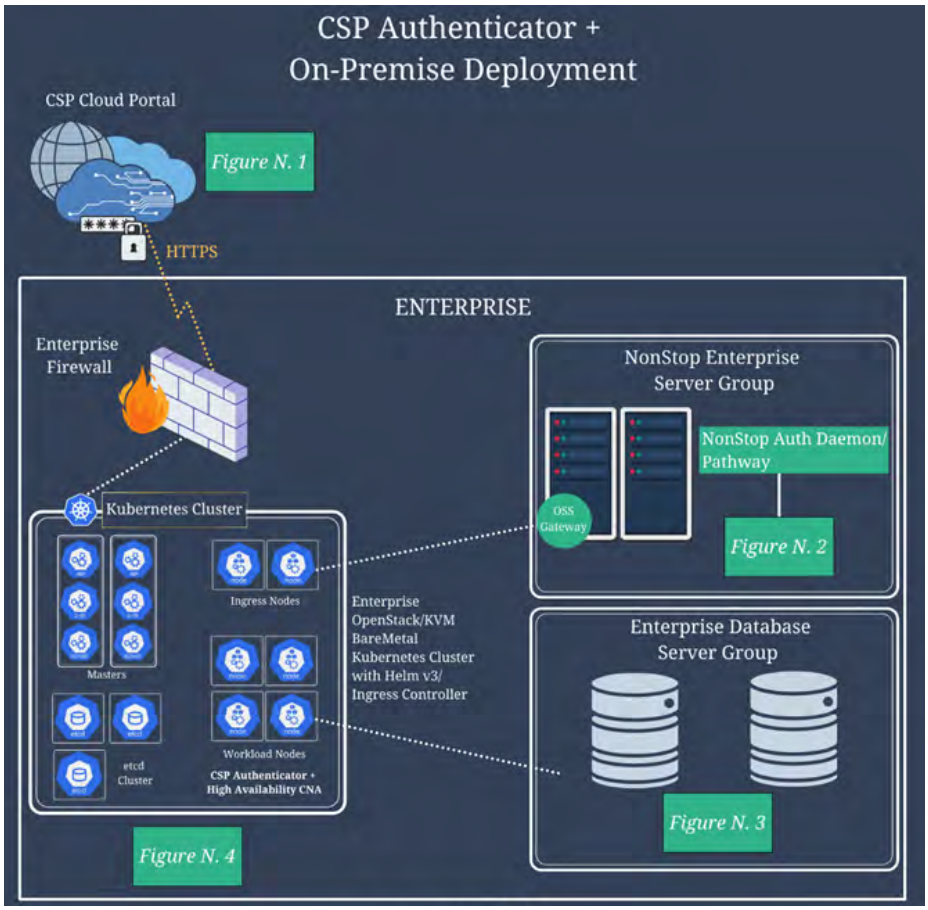
All communication with the CSP Authenticator+ cloud-native application is fully encrypted.

Key Features

- Support for multiple authentication factors including RSA, RADIUS, Active Directory, Azure, 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



In the diagram above

- Figure N.1 shows the CSP Cloud PortalTM, which contains the cloud licensing server, cloud services for biometric authentication, and additional user configuration options. The Cloud Portal is managed by CSP, but your firewall must allow outbound connections to the portal.
- Figure N.2 shows the CSP Authenticator + Agent, which must be installed on each NonStop server. The agent effectively enables multi-factor authentication for SafeGuard and Pathway applications. The CSP Authenticator + NonStop agent communicates with the CSP Authenticator+ High Availability Cloud-native Application (CNA) via CSP Gateway installed on the OSS system layer.
- Figure N.3 shows the customer-provided database which contains the CSP Authenticator + High Availability CNA. This database stores sensitive data and configuration settings, including authentication tokens, secrets, and other sensitive user information. The database may be located on-premise or in a cloud environment.
- Figure N.4 shows the High Availability Cluster. The CSP Authenticator+ High Availability CNA will be installed on this cluster and should be available via the DNS name chosen by the client.

Contact Us

comforte AG, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comforte, Inc., USA
phone +1 646 438 5716
ussales@comforte.com

comforte Asia Pte. Ltd.,
Singapore
phone +65 6808 5507
asiasales@comforte.com

comforte Pty Ltd, Australia
phone +61 2 8197 0272
aussales@comforte.com

www.comforte.com