PRODUCT BRIEF

MOBILE ENTRY POINT **(MEP)**

Enable secure remote access with granular controls for mobile users or third parties

Users work anytime and anywhere

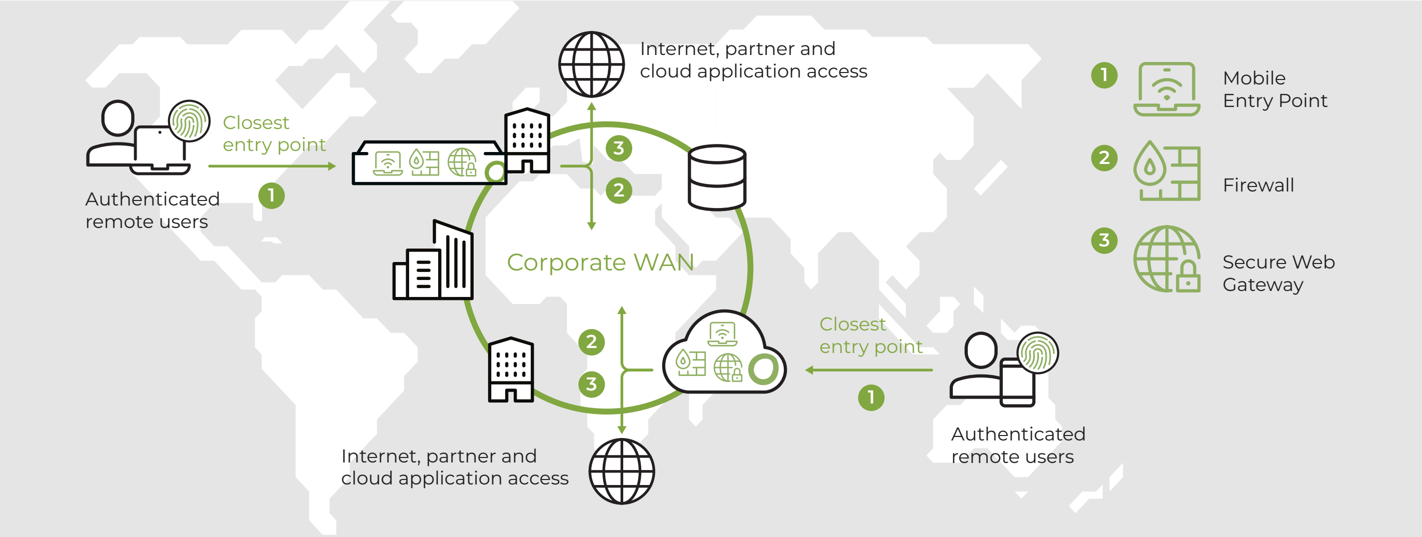
Users work anytime and anywhere these days. Hence, they need to have the possibility to seamlessly but securely access all internal resources independent of where they are.

Enforcing security policies is especially important for mobile users. In addition, users should be protected from internet threats when browsing on their corporate devices, even if they are traveling and are not in the office. Nevertheless, the user experience should not differ when connected remotely.

Mobile Entry Point as a secure access solution

The Mobile Entry Point service provides secure remote access for mobile users. Connected users can access corporate resources using an encrypted and easy-to-establish connection.

Open Systems Mobile Entry Point


Internet, partner and cloud application access
Closest entry point
Authenticated remote users
1
3
2
Corporate WAN
2
3
Closest entry point
1
Authenticated remote users
Internet, partner and cloud application access
1 Mobile Entry Point
2 Firewall
3 Secure Web Gateway

GLOBAL COVERAGE

By deploying Mobile Entry Points (Access Points) to existing or additional SD-WAN edge devices, global coverage can be provided for your mobile users.

Due to the deployment on SD-WAN edge devices, a reliable and secure connection to the corporate WAN is available.

SECURE ACCESS

Strong cipher suites and regular patching provide a secure connection from the remote users to the corporate WAN.

Enforce security policies on endpoints by activating “always-on” to block all network traffic on endpoints if they are not connected to a Mobile Entry Point.

EXPERT-LEVEL OPERATIONS

Enjoy the peace of mind of 24x7 monitoring, incident handling, and change management – provided by our L3 engineers.

Central policy setup and control allows you to enforce global security policies and configuration.

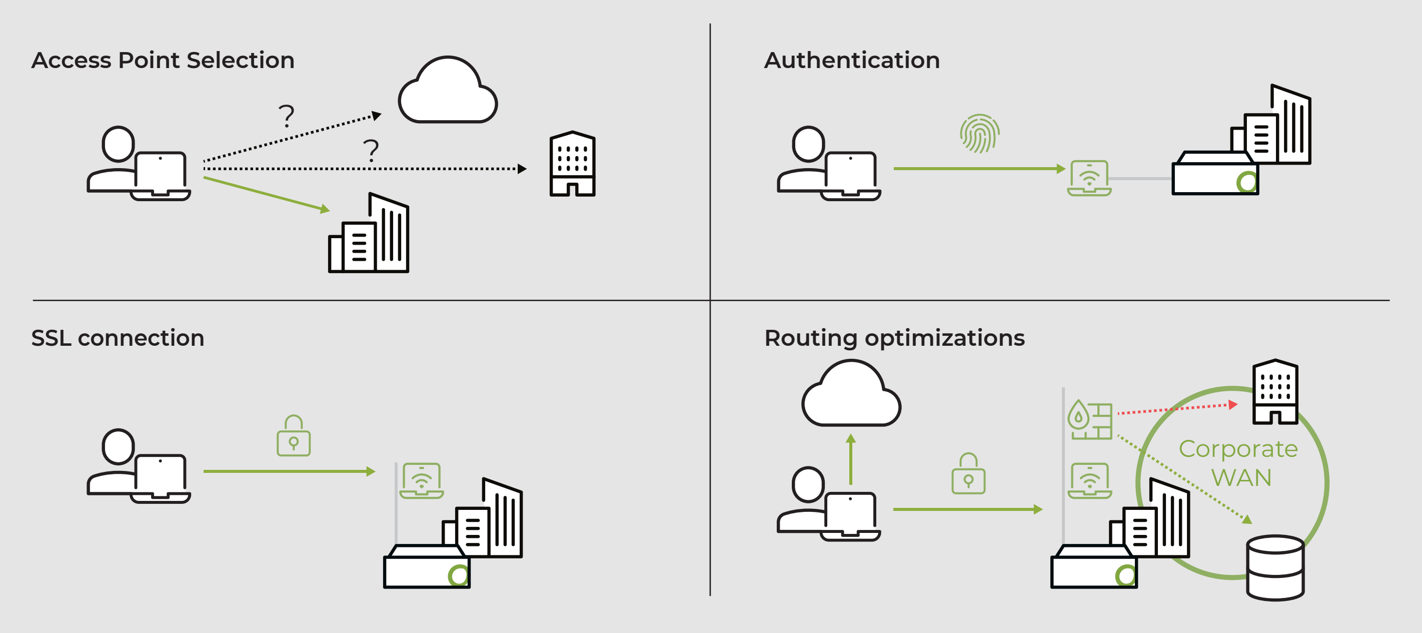
Mobile Entry Point: Secure Remote Access
How does the Mobile Entry Point solution work?

Access Point Selection: Either fixed, manually selectable or using a GeoDNS provider of choice, the right Mobile Entry Point is selected (on premises or in the cloud).

Authentication: Depending on a customer's requirements, authentication can either be done using username/password or a combination of user credentials and software/hardware tokens. Using certificates further improves the security or even allows seamless user authentication by using the certificate only.

Secure Connection: A secure and encrypted (DTLS) connection is established between the client and the Mobile Entry Point so that the exchanged traffic is encrypted and remains private.

Routing optimizations: Define routing policies for trusted applications to use the local internet breakout of the remote user or to allow access to the local LAN.



Corporate Access

Corporate Access supports an organization's mobile workforce and partner access by providing secure access to corporate network resources. It establishes a network-level connection, allowing clients such as personal computers, laptops, and mobile phones to access network resources from home or from anywhere in the world as if they were on site. Clients are authenticated according to the organization's policy. And access to corporate resources is restricted based on user groups.

Multi-factor authentication

Multiple authentication flows can be configured for different connections. In combination with the Identity Server, the users can be synced from the Windows Active Directory. Two-factor authentication can be used and managed in the Mission Control Portal. In combination with Azure AD/MFA or other Identity Providers, different authentication methods and levels are available to meet customers' requirements.

Open Systems connects and protects users, apps, and data everywhere they reside with a comprehensive, unified easy-to-use technology platform combined with an excellent 24x7 Managed SASE service.

Learn more at open-systems.com | Approved for public use. (CC, PM, May 2023)