

## Secure, Controlled Local and Remote Access

### AEP Series A Central Access Gateway

Concerned about network access? Have full control over what services, internal and external users can access, see or even know about. Protect all core assets from un-authorized access. Using AEP Series A Secure Application Access, managers can control authorised user access to resources and deny access to all other users. Series A provides a high level of granular access controls. Each user is presented with an icon-driven web portal of individual resources as defined by policy. Series A uniquely provides additional policy for Citrix XenApp and Windows RDS services by controlling resource allocation such as universal printing, audio resources, clipboard usage, drive mapping, and serial port redirection (easily set to “on/off” as needed).

Further, rather than providing users with a full desktop— which may represent a security risk in some instances — AEP Series A can present users with individual applications, eliminating the risks of users roaming the network. And, in addition to client health checks, it provides Client Machine Identification (CMID), allowing administrators to “fingerprint” a user’s device and “allow/deny” access accordingly.



## Key Capabilities

**Fine-Grained Access Controls:** Control access to URLs, applications, and data.

**Central Universal Access Solution:** One unit delivers secure, central access to all authorized applications regardless of server environment type (Windows RDS, Citrix XenApp, mainframe, and UNIX).

**Built-In Client Security:** Ensure remote computers adhere to corporate security policy. Verify the health and identity of client computers before allowing access.

**Ease of Use:** Familiar, icon-driven webtop delivers a single page for access to various desktop types.

**Easy to Set Up:** Web-based administration. Seamless connectivity with authentication and policy servers.

**Series A Virtual Edition available.** Choose from a hardware or virtual solution.

## Security Features

SSL encryption for secure connections.

Strong, two-factor authentication support (RSA, VASCO— built in server).

**Application Layer Proxy**— Applications remain safe on the server and are never directly exposed to the public network.

**Device Fingerprinting** — Limits access to pre-approved client devices.

**No new firewall ports** – SSL traverses standard https ports already open for Web traffic.

**Layered Authentication** — Flexible, V-realm framework combines numerous protocols: RSA SecurID®, LDAP, Windows® NT®, RADIUS, Windows Active Directory, Kerberos, ActivCard (Smart Cards), and more.

**FIPS 140-2 Level 4 option** — Security at the highest FIPS level.

#### United States

Toll-Free: +1-877-638-4552  
Tel: +1-732-652-5200

Email: [sales@aepnetworks.com](mailto:sales@aepnetworks.com) Web: [www.aepnetworks.com](http://www.aepnetworks.com)

#### Europe

Tel: +44 1344 637 300

#### Greater China

Tel: +8621 5116 7120

#### SE Asia, Singapore

Tel: +852 2961 4566

#### Japan

Tel: +8180 5645 4503

#### Australia/New Zealand

Tel: +61 2 9413 2282

#### Malaysia

Tel: +60 32166 2260