

Ten Keys for Secure Remote User Access

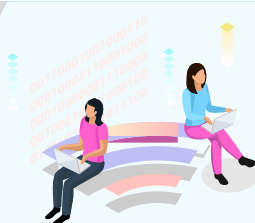


Secure remote access plays a vital role for organizations who strive for a accessible, zero down time, environment. When considering business continuity plans and disaster recovery measures, organizations must be flexible and offer their remote workforce a platform to synchronize activities performed with on-premise counterparts as well as a means to access their virtual applications and desktops.

With the AmZetta Digital Workspace (DWS), you can appease both your on-premise and your remote workforce with a single unified solution to ensure that regardless of where a user is or what they are accessing, your environment is secure and safeguarded to mitigate threats while boosting availability for your users.

AmZetta's Digital Workspace (DWS) solution is the amalgamation of many advance technologies such as: a Virtual Desktop Infrastructure (VDI) for managing virtual applications and desktops, a Zero-Trust based gateway for secure remote access (ZTNA), an integrated identity management suite for user monitoring, a multi-factor authentication (MFA) controller for validation, and data leakage protection to keep your data safe and contained. AmZetta has tightly integrated each of these components under a single solution to reduce susceptibility and management strain while boosting your company's revenue, user satisfaction, and employee productivity!

Ensure business as usual



Keep your critical business functions active and running by providing secure remote access to internal or cloud based virtual applications and desktops. Allow remote users to securely access assigned network resources with contextual based security measures and containerization, ensuring that users are safe to access data from anywhere and from any device.

Deliver zero trust access to all apps

Improve your employee experience by providing your remote workforce with robust and reliable access through a multi-factor authentication (MFA) controller to validate devices and users seamlessly. And with Zero-Trust Network Access (ZTNA) you can rest assure that individuals access only what their assigned to.





Prevent data leakage in remote endpoints

Allow access only from compliant devices. Block data download, copy-paste, print-screen, screen recording, printing features and control users' internet access.



Enable secure remote access

Securely and seamlessly access business applications anytime, from anywhere, using any device, without exposing internal network to external threats.

Empower BYOD users

Allow your users to utilize any device: laptop, thin client, mobile, etc, without compromising your security or hindering workflow.



Deliver graphical workstations remotely

Enable your users with graphically intensive desktops and applications no matter where they are. Allow users to analyze and render large data sets without the hindrance of resource limitations.

Deliver audio in high quality over the internet

Provide high quality audio to remote users through a secure tunnel that works well even over low bandwidth networks.





Comply with regulatory norms

Comply with RBI, GLBA, FFIEC, HIPAA, EPCS, other data security, and privacy regulations by providing contextual and risk-based remote access to users. Make use of detailed audit logs to get insights into user activities. Use multiple parameters like log-in time, device location, device fingerprint, etc., to bind the user to a single authorized device. Also enable strict data leakage prevention policies.

User experience

The App tunneling feature routes only the traffic from the device to the associated application, whereas web traffic is sent directly to the internet for increased performance.



Seamless deployment

As an identity-based solution, the integration with existing directory services enables rapid deployment and management of policies.

Interested in testing Digital Workspaces in Your Environment?

Just click the link below, input your name and email ID. We will send you the URL, username and password to evaluate the Digital Workspace solution. <https://amzetta.com/demo/>



©2021 AmZetta Technologies, LLC. All rights reserved. zPortal™, zGateway™, zBrows™ and zMFA™ are either registered trademarks or service marks or trademarks or service marks of AmZetta Technologies, in the United States and/or other countries. Any other trademarks are the properties of their respective owners. v.230221

AmZetta Technologies
5555 Oakbrook Parkway,
Suite 280
Norcross, GA 30093

Technical Support
support@AmZetta.com
1-800.892.6625

Sales & Product Info
sales@AmZetta.com
1-877.991.1809
<https://amzetta.com>