accops

Accops Digital Workspace

Unleash true work-from-anywhere flexibility by securely delivering applications or complete desktop environments to every user—employees, field teams, and management—establishing a compliant, high-performance digital workspace.

BROCHURE

Accops Digital Workspace

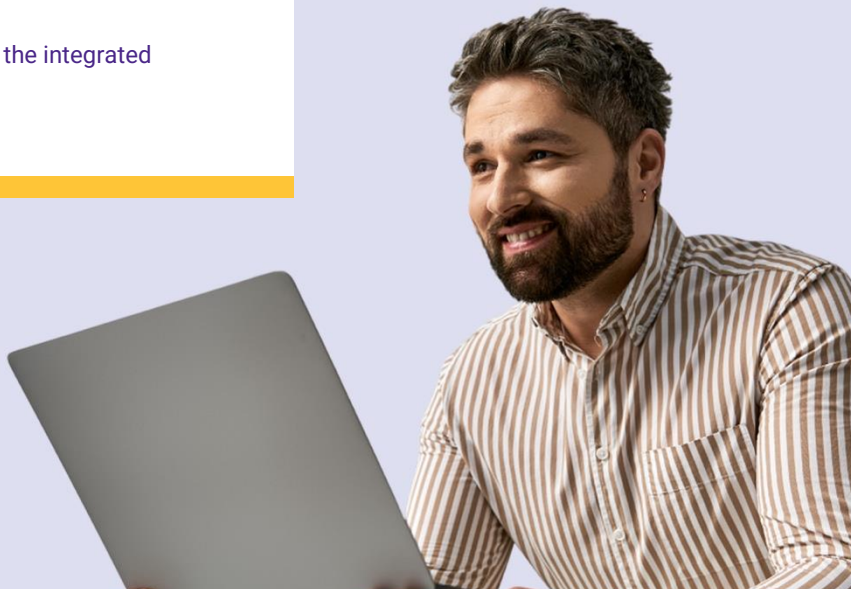
Accops Digital Workspace helps organizations create a future-ready, compliant workspace and empower their workforce to be at their productive best wherever they are. Accops Digital Workspace provides a comprehensive, zero-trust-based end-user computing solution, enabling instant secure access to business applications from anywhere, any device and any network.

The Accops solution suite includes End-user Computing Virtualization via application & desktop virtualization (VDI), zero trust-based Application Access Gateway and Identity & Access Management solutions. It's an end-to-end integrated solution that takes care of remote access, application virtualization, VDI, MFA, identity federation, SSO and thin client needs, sparing organizations the need to juggle multiple product points from different vendors.

Accops Digital Workspace solution is highly modular to fit the needs of businesses of all sizes, providing seamless access to modern web applications, SaaS applications, client-server applications, legacy applications, virtual applications and virtual desktops.

Accops Digital Workspace is an integrated solution to take care of remote access, VDI, MFA, identity federation, SSO & thin client needs

- Provide instant access to business applications from anywhere, using any device
- Replace conventional devices with smart, green thin client
- Control every device, application & OS and prevent security breaches
- Reduce TCO and optimize OpEx using the integrated offering



Key Features

Virtual Desktop Provisioning

Accops Digital Workspace solution supports both session-based desktops as well as dedicated virtual desktop-based VDI. Administrators can add a Microsoft RDS server for session-based desktop. Dedicated virtual desktops can be created, managed and delivered by adding VMWare vCenter, VMWare ESX, Microsoft Hyper-V or SCVMM. Linked-clones as well as full clones for VMWare-based platform can also be created. It is possible to enable SysPrep from Accops console, enabling administrators to provision hundreds of virtual desktops with merely a few clicks.

Zero Trust-Based Remote Access

Accops Digital Workspace uses Secure Private Application Network (SPAN) technology to enable a high performance, simplified remote access deployment. Accops' SPAN technology enables remote and mobile users to access business applications from any device, even over slow networks with high latency. Accops solution detects, scans and evaluates the trust level of all endpoints, based on which, access is provided. Internet access on end user machine can also be controlled and restricted based on user role and responsibilities.

Strong Endpoint Control

Before an end user is allowed to access the applications, Accops Digital Workspace lets organizations detect, scan and evaluate the trust level of the device used by the user. Based on the trust level, access from the device can be controlled and restricted. Accops solution has the feature to detect the device location and implement different security policies based on the location of the device.

Integrated Application Delivery

Accops Digital Workspace makes application delivery to end-users simple. Administrators can source applications from different sources, like applications installed on Microsoft RDS server, Microsoft App-V or through application streaming products, and deliver the subset to end users. The applications get seamlessly integrated to user's PC, virtual desktop of the user or are available in the user portal. User can access these applications using any device they use.

Built-in Identity & Access Management

The built-in Identity and Access Management solution safeguards critical business applications and data from misuse by internal as well as external users, by managing user identities and monitoring user access. Organizations can have strong control over endpoints by enabling contextual access, device entry control and flexible policy framework. The out-of-the-box MFA is compatible with all applications. It enables strong authentication through multiple token options – SMS, Email, mobile app, PC software – or facial and fingerprint-based biometric authentication. Single sign-on (SSO) feature provides better security and convenience. Accops Digital Workspace can also generate alerts if access to any corporate application by a user breaches the set risk thresholds, enabling organizations to detect and prevent identity thefts and credential sharing.

Detailed Auditing & Logging

Accops Digital Workspace provides administrators with detailed reports on all activities within the corporate environment. It provides detailed logs on who accessed what, when & from where along with end-device details.

Secure Sandbox Computing

With Accops Digital Workspace, organizations can create a secure sandbox for end user computing. In the secure sandbox, the user can be restricted to run limited applications and they can be restricted from copying data from applications to local system or take data out of their machines. The secure sandbox can control clipboard, printing, desktop session recording, file saving, USB access, and internet access, among others. Based on the user location, the sandbox can adjust itself to relax the restrictions if the user is working from a trusted location.

Device Management

When a PC running Accops client or a thin client is available on network, the device automatically registers itself with the Accops controller and is available for management from the console. Administrator can view the status of the device, sessions and modify the device properties. Administrator can also push updates to the devices as and when they are available. Alerts management

can be done from the central console for devices which require extra attention.

Seamless, Safe Enterprise Mobility

Accops Digital Workspace comes with the latest TLS protocol-based data security and integrity for application traffic. By deploying Accops Digital Workspace, organizations can secure any business application and make it available to end users without any pre-configuration on end users' machines. Organizations can also easily enable extranet users, vendors, consultants to bring their own device for application access.

User Productivity & User Experience Monitoring

Accops Digital Workspace enables organizations to monitor productivity of their distributed workforce with per-user data points, like log on time, log out time, and the time for which the user accessed each application. It is capable of providing regular automated email updates with per-user details, like total session time, application access time, etc., which can be used by HR teams for productivity measurement. The response time of each application can be identified and the issues with slower applications can be acted upon, to provide better user experience.

Privilege Access Audit & Control

Organizations can track, control and audit privilege access by the IT teams, support teams, developers and consultants who need administrative privilege to systems for their regular work. Accops Digital Workspace helps organizations mitigate all potential security concerns posed by privilege access, by enabling them to accurately track all details of privilege user accounts usage.

Scalable, Reliable & Highly Available

With built-in Load Balancing and high availability features, Accops Digital Workspace can be scaled to thousands of users to ensure required uptime for business-critical operations. Accops Digital Workspace has built-in load balancing for incoming users, as well as application traffic to ensure that the deployed hardware is effectively used. HySecure can be setup in DR mode with client side failover feature so that end users can always connect, ensuring uninterrupted access to applications and data.

Datasheet

CATEGORY	DETAILS

Application & Virtual Desktop Publishing	• Session-based Applications & Desktops
	  ○ Microsoft Windows RDS Server , 2016, 2019, 2022, 2025
	• Ubuntu-based terminal server
	• Dedicated Virtual Desktop OS
	  ○ Windows: Microsoft Windows 10/11
	  ○ Linux: Ubuntu 22, RHEL v9

Hypervisor Support	• VMware ESXi 5.5 or above • VMware vCenter 5.5 or above • Nutanix AHV/Prism Central • Microsoft Hyper-V 2012 R2/2016/2019/2022 • Microsoft SCVMM 2012 R2/2016/2019/2022 • Cloud: Microsoft Azure • Physical Desktops
Application Support	• All web-based, TCP and UDP based client server applications • Windows file shares and drive mapping • Dynamic port-based applications • Publish subnet or IP range for network access

	• Special support for RDP virtual channels • Application server load balancing • Session caching for load-balanced applications • VoIP (Voice over IP) • FTP • Fileshare • Per application-based compression switch • MyDesktop for direct personal desktop access • HyWorks VDI and Hosted Application • o365, GSuite, Salesforce (MFA is supported)
Device Management	• Display configuration • Device setting like volume USB ports • USB port redirection driver management • Device lock down settings • Device UI option security and control • Device power save settings • Language and keyboard settings • Device diagnostics settings and log collection • Grouping of devices for easier management • Wizard driven installation procedure • Certificate-based strong authentication for administrators • Web-based management console

System Management	• Logging & reporting
	  ○ Log achieving
	  ○ Users logs, admin logs, device logs, alerts
	• Automated & manual configuration backup
	• Cluster management
	• Session host server management*

Application Publishing Features	• Remote browser application • Application folder support • Application shortcut publishing • Customer icon publishing • Launch in single session
Session Policies	• Protocol performance control • Universal printing • Printing quality control • Printing bandwidth control • Clipboard control • Drive mapping control
Desktop Provisioning	• Full clones • Permanent and temporary Desktops • Power management for virtual desktops • Auto-expand pool • Desktop customization using SysPrep • Recompose desktops using source VM • Virtual desktop target location management

	• Persistent & non-persistent desktops
Entitlements	• HyDesk (Thin client) device • PC with HyDesk client • User Identity • GroupOU • Shared desktop assignment • One-to-One assignment • Auto-assign desktops on first login • Permanent or temporary assignment
Endpoint Control	• Strong device identification based on 20 parameters includes CPUID, MBID, HDDID, MacID, IMEI number and more • Detect managed and unmanaged devices • Login control from managed and unmanaged devices • Support for checking for antivirus, firewall, antispyware products • Real-time status check for last update time • Real-time protection check • Application control based on device • Mandatory profile for non-avoidable policy checks on all endpoints • Quarantine profile for devices that fails all other profiles • Secure endpoints from attacks over internet or becoming a proxy for attacks • Restrict user access to the user based policy, printing, USB devices • Geolocation-based restriction • Windows update-based restriction • Profile-based security policy
Network Security	• Version upto TLS1.2, Encryption: Strongest available – DES, 3DES, AES • Authentication: SHA-2, RSA 2048, 4096 bit RSA key CA Certificate support • Internet network masking and IP address/hostname mangling • Application level gateway and not layer 2 bridging • Hardened gateway operating system • Split & full tunnel access modes • Secure sandbox computing • DDOS Protection
Access Methods	• HyDesk devices • HyWorks client for PC on Microsoft Windows, Ubuntu & macOS • HySecure client for PC on Microsoft Windows, Ubuntu & macOS • HyWorks client SDK for thin client integration • iOS & Android app • Hybrid portal mode • Portal with Java applications • Accops Nano LIVE USB • Accops HyLite Web portal for clientless access • L3 mode • Reverse proxy clientless VPN for web applications • Site-to-site access

Monitoring, Logging, Auditing	• Monitor device availability status • Monitor session status with details on CPU usage and power consumption • Monitor idle session status • Timeout idle sessions automatically • Manually terminate sessions • Virtual desktop power status • Manage power operations • Authentication server reachability status • Hypervisor reachability status • Resource utilizations • Session recording • Customizable graphical dashboard & reports with detailed event collection, real-time visibility, email alerts & reports • Watermark with date, time and customizable logo, text, username for Virtual Apps & Desktops • List of all applications and duration for which each application was running • Support for external SIEM servers • Logs of information like time of access, username, domain name, MAC address of endpoint, IP address of endpoint, application accessed, device profile, file uploaded/downloaded • Reporting on domain wise access, applications accessed, failed login attempts, concurrence graph • Alert on Resource Utilization • Productivity logs • User location monitoring and impossible travel notification • Monitor users for log monitoring • Sys log report • Detailed logging of endpoint security scans results • Complete reporting of user logons and activity
Deployment	• Scalable to thousands of users • Active-Active N+1 cluster • Application connection load balancing • Session persistence: Users do not need to re-authenticate • ISP load balancing for incoming connections • Client side failover using alternate gateways • Runs on hardened Linux based platform • Menu driven console interface for easy configuration • Can run on any standard or custom hardware • Hyper-V virtualization platforms from VMware, XenServer, Hyper-V

Authorization	• Application-based access control
	• Access control based on
	  ○ Device identity and profile
	  ○ Endpoint security trust level
	  ○ User authentication method
	  ○ User role
	  ○ User's organization
	• Dynamic policy evaluation based on run time information about device, authentication method and user role
	• Display of allowed applications and availability of the application server to users
	• Time based restriction policies
	• Scheduled account expiry
	• Block specific groups
	• Multiple VPN Domain based control
	• Control user internet access
	• Support for external authorization servers
	• Automatic expiry of ACL (Access Control List)
	• Authentication based on
	  ○ User identity, OU/group/realm
	  ○ Static passwords, OTP – dynamic passwords
	  ○ Certificates
	  ○ Device Signature: CPUID, HDDID, MacID, IMEI No., and more
	  ○ User location, IP address
	  ○ Endpoint security trust level
	• 2FA based on certificates, device signatures
	• OTPs through SMS/Email/Hardware/Software Token
	• Local database with full customization per user, password policies, password reset support
	• RSA secure ID or 3rd party OTP server
	• Integrates with AD/LDAP/RADIUS/SAML/ pre-existing biometric authentication server
	• Fully integrated client-certificate based 2FA server with automatic CA and certificate provisioning
	• Novell e-Directory
	• SSO NPM-based apps
	• SSO-based SAML
	• Consent (Push Notification)
	• Consent with additional tokens (Push Notification)
	• Support for FIDO & Passwordless Logon
	• Biometric Authentication

Redefine the way your enterprise works with Accops Digital Workspace — unifying application delivery, secure access, and identity management into one cohesive, compliant platform.

Future-proof your business with a secure and agile solution designed for scale. Connect with us at contact@accops.com to begin your transformation.