



Digital Workspace



Digital Workspace

Transform your business with a compliant and integrated solution

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 a one 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 one 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.

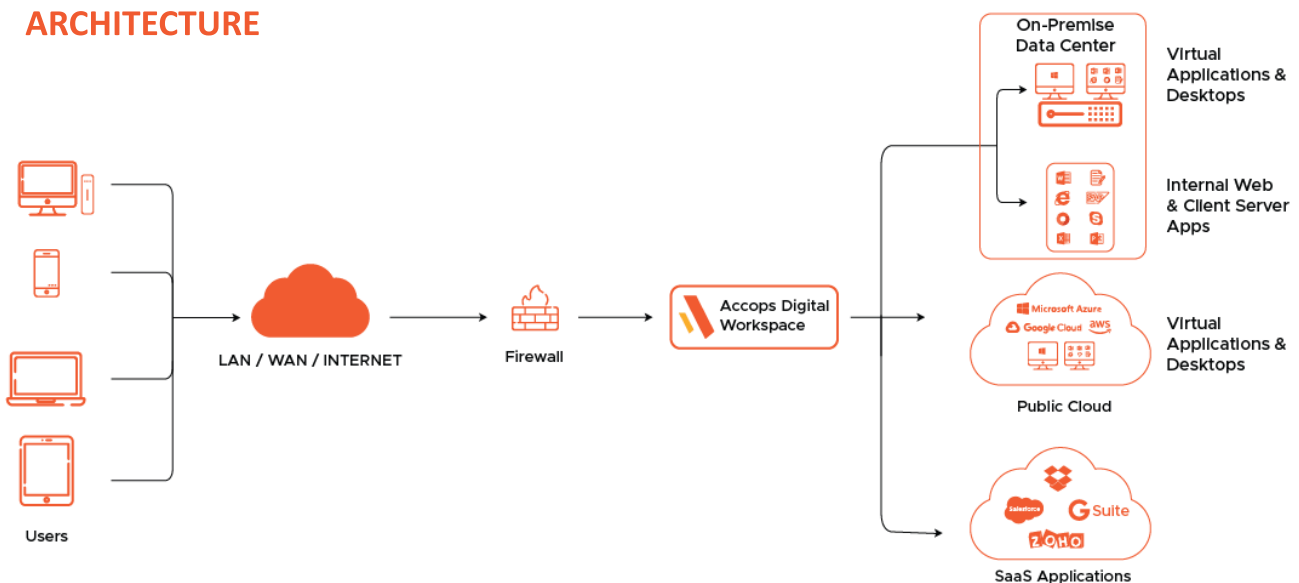
Privilege Access Audit & Control

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 help 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.

ARCHITECTURE



DATASHEET

Application & Virtual Desktop Publishing	Desktop Provisioning
Session-based Applications & Desktops	Desktop Pools
• Microsoft Windows RDS Server 2008 R2 – SP1, 2012 R2, 2016, 2019	Full and limited clones
• Ubuntu-based terminal server	Permanent and temporary Desktops
Dedicated Virtual Desktop OS	Power management for virtual desktops
• Windows: Microsoft Windows 7/8/10	Auto-expand pool
• Linux: Ubuntu & CentOS	Desktop customization using SysPrep
Hypervisor Support	Recompose desktops using source VM
VMWare ESXi 5.5 or above	Virtual desktop target location management
VMWare vCenter v5.5 or above	Persistent & non persistent desktop
Nutanix AHV/ Prism Central	Entitlements
Microsoft Hyper-V 2012 R2/2016	HyDesk (Thin client) device
Microsoft SCVMM 2012 R2/2016	PC with HyDesk client
Cloud: Microsoft Azure	User Identity
Physical Desktops	Group/OU
Application Support	Shared hosted desktop assignment
All web-based, TCP and UDB based client server applications	One to One assignment
Windows file shares and drive mapping	Auto-assign desktops on first login
Dynamic port-based applications	Permanent or temporary assignment
Publish subnet or IP range for network access	Endpoint Control
Special support for RDP virtual channels	Strong device identification based on 20 parameters includes CPUID, MBID, HDDID, MacID, IMEI number and more
Application server load balancing	Detect managed and unmanaged devices
Session caching for load-balanced applications	Login control from managed and unmanaged devices
VoIP (Voice over IP)	Support for checking for antivirus, firewall, antispymware products
FTP	Real-time status check for last update time
Fileshare	Real-time protection check
Per application-based compression switch	Application control based on device profile
MyDesktop for direct personal desktop access	Mandatory profile for non-avoidable policy checks on all endpoints
HyWorks VDI and Hosted Application	Quarantine profile for devices that fails all other profiles
o365, Gsuite, Salesforce (MFA is supported)	Secure endpoints from attacks over internet or from becoming a proxy for attacks
Device Management	Restrict internet access of the user based on policy
Display configuration	Restrict users from accessing clipboard, printing, USB devices
Device setting like volume USB ports	Geolocation-based restriction
USB port redirection driver management	Windows update-based restriction
Device lock down settings	Profile-based security policy
Device UI option security and control	Access Security
Device power save settings	TLS 1.0, 1.1, 1.2 and above
Language and keyboard settings	Encryption: Strongest available – DES, 3DES, AES
Device diagnostics settings and log collection	Authentication: SHA-2, RSA 2048, 4096
Grouping of devices for easier management	4096 bit RSA key CA Certificate support
Wizard driven installation procedure	Internet network masking and IP address/hostname mangling
Certificate-based strong authentication for administrators	Application level gateway and not layer 2 bridging
Web-based management console	Hardened gateway operating system
System Management	Split & full tunnel access modes
Logging & reporting users logs, admin logs, device logs, alerts	Secure sandbox computing
Log achieving	DDOS Protection
Automated & manual configuration backup	Access Methods
Cluster management	HyDesk devices
Session host server management*	HyWorks client for PC on Microsoft Windows, Ubuntu & macOS
Application Publishing Features	HySecure client for PC on Microsoft Windows, Ubuntu & macOS
Remote browser application	HyWorks client SDK for thin client integration
Application folder support	iOS & Android app
Application shortcut publishing	Hybrid portal mode
Customer icon publishing	Portal with Java applications
Launch in single session	Accops Nano Live USB
Session policies	Accops HyLite Web portal for clientless access
Protocol performance control	L3 mode
Universal printing	Reverse proxy clientless VPN for web applications
Printing quality control	Site to site access
Printing bandwidth control	
Clipboard control	
Drive mapping control	

DATASHEET

Monitoring, logging, auditing	Authorization
Monitor device availability status	Application-based access control
Monitor session status with details on CPU usage and power consumption	<i>Access control based on</i>
Monitor idle session status	<ul style="list-style-type: none"> • Device identity and profile • Endpoint Security trust level • User authentication method • User role • User's organization • User's location
Timeout idle sessions automatically	
Manually terminate sessions	
Virtual desktop power status	
Manage power operations	
Authentication server reachability status	Dynamic policy evaluation based on run time information about device, authentication method and user role
Hypervisor reachability status	
Resource utilizations	Display of allowed applications and availability of the application server to users
Session recording	
Customizable graphical dashboard & reports with detailed event collection, real time visibility, email alerts & reports	Time based restriction policies
Watermark with date, time and customizable logo, text, username for Virtual Apps & Desktops	Scheduled account expiry
Logs of all applications and duration for which each application was running	Block specific groups
	Multiple VPN Domain based control
Support for external SIEM servers	Control user's Internet access
	Support for external authorization 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	Automatic fetching of group information from AD/LDAP/RADIUS
	Automatic expiry of ACL (Access control List)
	Authentication
Reporting on domain wise access, applications accessed, failed login attempts, concurrence graph	<i>Authentication based on</i>
Alert on Resource Utilization	<ul style="list-style-type: none"> • 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
Productivity logs	
User location monitoring and impossible travel notification	
Monitor users for log monitoring	
Sys log report	
Detailed logging of endpoint security scans results	2FA based on certificates, device signatures
Complete reporting of user logons and activity	OTPs through SMS/Email/Hardware/Software Token
Deployment	Local database with full customization per user, password policies, password reset support
Scalable to thousands of users	RSA secure ID or 3 rd party OTP server
Active-Active N+1 cluster	Integrates with AD/LDAP/RADIUS/SAML/ pre-existing biometric authentication server
Application connection load balancing	
Session persistence: Users do not need to re-authenticate	Fully integrated client-certificate based 2FA server with automatic CA and certificate provisioning
ISP load balancing for incoming connections	
Client side failover using alternate gateways	Novell E-Directory
Runs on hardened Linux based platform	SSO NPLM-based apps
Menu driven console interface for easy configuration	SSO-based SAML
Can run on any standard or custom hardware	Consent (Push Notification)
Runs on virtualization platforms from VMware, XenServer, Hyper-V	Consent with additional tokens (Push Notification)
	Support for FIDO & Passwordless Logon
	Biometric Authentication

ACCOPS PRODUCT EDITIONS

	FEATURES	HyWorks Silver	HyWorks Gold	Virtual Browser	Digital Workspace Silver	Digital Workspace Gold	Digital Workspace Platinum	HyLabs	HyLite	HySecure Silver	HySecure Gold	HySecure Platinum	HyID Silver	HyID Gold	HyID Platinum
A	End User Computing Virtualization														
1	Windows Server based Personal Virtual Desktop (Server 2008 R2, 2012 R2, 2016, 2019)	x	x	x	x	x	x								
2	Windows Server based Shared/Pooled Virtual Desktop (Server 2003, 2008, 2008 R2, 2012 R2, 2016, 2019)	x	x	x	x	x	x								
3	Windows Server based Virtual Applications (Server 2008 R2, 2012 R2, 2016, 2019)	x	x	x	x	x	x								
4	Windows 10/8/7 based Personal Virtual Desktop	x	x		x	x	x	x							
5	Windows 10 based Shared/Pooled Virtual Apps & Desktop in Azure	x	x		x	x	x								
6	Windows 10 based Virtual Applications	x	x		x	x	x								
7	Linux based Personal Virtual Desktop		x	x		x	x	x							
8	Linux based Shared/Pooled Hosted Desktops (Server 2008 R2, 2012 R2, 2016, 2019)		x	x		x	x	x							
9	Linux based Virtual Applications (Ubuntu 16 & above, CentOS 7 & above, RHEL 7.5 & above)		x	x		x	x	x							
10	Remote access to physical PCs: dedicated/floating pool management		x			x	x	x							
11	Virtual Training Lab provisioning, management, and access						x	x							
B	Infrastructure Support														
1	Support for flexible desktop pool deployment: Personal, Pooled, Floating, Fixed, Persistent, non-Persistent	x	x	x	x	x	x	x							
2	Support for on-premise VMWare vSphere, Nutanix AHV, Microsoft Hyper-v, Microsoft SCVMM with complete VM provisioning, power management and monitoring for delivering virtual apps & desktops.	x	x	x	x	x	x	x							
3	Support for KVM, Xen, GCP for Virtual apps & pooled shared desktop delivery	x	x	x	x	x	x	x							
4	VM provisioning automation using linked cloning function for VMWare vSphere & Microsoft Hyper-v with SCVMM including recompose	x	x	x	x	x	x	x							
5	Support for Azure WVD with complete VM provisioning, power management, and monitoring for delivering virtual apps & desktops.	x	x	x	x	x	x	x							
6	Support for AWS Cloud with complete VM provisioning, power management, and monitoring for delivering virtual apps & desktops and with dynamic power management with customized per day plan to save on AWS cost.	x	x	x	x	x	x	x							
7	Support for dynamic power management with customized per day plan to save on Azure cost.	x	x	x	x	x	x	x							
8	Connect via Hyper-v or VMWare console (experimental) to support users with full tunnel VPN client inside VDI		x			x	x								
C	Application Support														
1	Support for Web browser virtualization for Internet isolation: Chrome, Internet Explorer, Firefox and more	x	x	x	x	x	x								
2	Support any Windows or Linux based application	x	x		x	x	x								
3	Support for lab virtualization with time-based scheduling of virtual desktops							x							
4	Support for graphics rich apps, 2D apps and light weight 2D applications with or without having a vGPU in the VM using Microsoft RemoteFX	x	x	x	x	x	x	x							
5	Support for heavy graphics applications by utilizing vGPU on the virtual machines for virtual apps and desktop (Needs PCoIP license for better display performance)		x*		x*	x*	x*	x*							

	FEATURES	HyWorks Silver	HyWorks Gold	Virtual Browser	Digital Workspace Silver	Digital Workspace Gold	Digital Workspace Platinum	HyLabs	HyLite	HySecure Silver	HySecure Gold	HySecure Platinum	HyID Silver	HyID Gold	HyID Platinum
D	Virtual apps & desktop security management														
1	Secure File upload/download work flow with detailed audit logs: one way file transfer, file type control, file size control		x	x	x	x	x								
2	Application containerization and sandboxing for virtual apps & applications within virtual desktops, based on user and device context						x								
3	Virtual IP address for each user session for pooled desktop or virtual apps users		x	x		x	x								
4	Application isolation using MSIX packages with efficient one click application delivery		x			x	x	x							
5	User profile management using FSLogix and UPD	x	x	x	x	x	x	x							
6	Contextual Application access and application sandboxing for virtual apps & virtual desktops		x			x	x								
E	Session Experience Management														
1	Accops Shell for virtual desktops	x	x	x	x	x	x	x							
2	Session policies to control user experience and permissions, customizable at user, group, OU, server, VM and device level	x	x	x	x	x	x								
3	User session performance management with CPU overuse control and application resource allocation management		x	x	x	x	x								
4	User Experience Monitoring and Management		x			x	x								
5	Self-Service for Users for Session performance management		x			x	x								
F	Local Resource Redirection and Session Experience														
1	Driverless printing via Accops HyPrint driver for any modern and legacy application (PDF, Text based printer)	x	x	x	x	x	x	x							
2	Support for eTokens for digital certificate signing on Windows or Linux based virtual apps and desktops	x	x	x	x	x	x	x							
3	Seamless USB peripheral redirection for virtual desktops and virtual apps running on personal virtual desktops with Windows 10 or Linux	x	x	x	x	x	x	x							
4	Enhanced USB peripheral redirection for pooled virtual desktops and virtual apps running on Microsoft RDS Server (Needs additional License for enhanced USB redirection module)	x*	x	x*	x*	x*	x	x*							
G	Access to Virtual Apps & Virtual Desktops														
1	Accops Desktop client to access Virtual apps and Virtual Desktop: Windows 7/8/10, macOS, Ubuntu 16 & higher, CentOS 7 & higher, Bharat OS, Windows 10 IoT	x	x	x	x	x	x	x							
2	Accops Integrated portal to access Virtual apps and Virtual Desktop: Windows 7/8/10, macOS, Ubuntu 16 & higher, CentOS 7 & higher, Bharat OS, Windows 10 IoT			x	x	x	x	x							
3	Accops Workspace client for iOS & Android to access virtual apps & desktops and Microsoft RDP based connections inside Accops container			x	x	x	x	x							
4	Clientless access to Virtual Apps & Desktops using HTML5 supported browser (HyLite)			x	x	x	x	x	x						
5	Seamless file transfer, endpoint security, USB redirection and other advanced features for Clientless portal using HTML5 browser			x		x	x		x						
6	Remote access to Virtual Apps & Desktop via Accops HySecure			x	x	x	x	x	x						
I	Management, Reporting & Compliance for Virtual Apps & Desktop														
1	Productivity Monitoring on virtual apps & desktops including time spent on each application		x	x	x	x	x								
2	Session Recording for Virtual Apps & Desktops		x			x	x								
3	Watermark for Virtual Apps & Desktops		x		x	x	x		x						

	FEATURES	HyWorks Silver	HyWorks Gold	Virtual Browser	Digital Workspace Silver	Digital Workspace Gold	Digital Workspace Platinum	HyLabs	HyLite	HySecure Silver	HySecure Gold	HySecure Platinum	HyID Silver	HyID Gold	HyID Platinum
4	Built-in reports and support for external SIEM servers	x	x	x	x	x	x	x	x						
5	Customizable dashboard & reports with detailed event collection, email alerts and reports in email. (Needs additional license for Accops Reporting Server)		x*	x*	x*	x	x	x*	x*						
6	Multi-tenancy support to manage multiple organizations from single deployment		x*	x*	x*	x	x	x*	x*						
7	Time based access to apps & resources with notifications to alert admin of expiring ACLs			x	x	x	x	x	x						
8	Multiple high availability deployment support including Active-Passive, Active-Active	x	x	x	x	x	x	x	x						
9	Support for Disaster recovery sites with automated customizable data synch	x	x	x	x	x	x		x						
10	Support Microsoft SQL Express edition for up to 2000 concurrent user deployment. Supports paid SQL editions	x	x	x	x	x	x								
11	Record resource consumption at each server, session and user level and provide detailed reports		x	x	x	x	x								
12	Centralized web based management console with dashboards	x	x	x	x	x	x								
J	Remote Access to Private Applications														
1	Integrated workspace access portal to access any private applications (web apps, client-server apps, virtual applications and virtual desktops), Cloud Apps, SaaS applications. (Note: Virtual apps & desktops needs separate licensing)				x	x	x			x	x	x		x	x
2	Accops Workspace client for Windows, macOS & Linux for accessing web apps, client-server apps, SaaS apps, virtual apps & desktops from a single user interface: Windows 7/8/10, macOS, Ubuntu 16 & higher, CentOS 7 & higher, Bharat OS, Windows 10 IoT				x	x	x			x	x	x			
3	Secure Remote Access gateway with Accops SPAN technology based on application tunnels to create Zero trust-based access gateway and using latest TLS 1.3/1.2 protocol with latest cipher support				x	x	x			x	x	x			
4	Secure Remote Access gateway with Accops Turbo technology to create a seamless network extension based on Datagram based tunnel and latest cipher support				x	x	x			x	x	x			
5	Accops Workspace client for iOS & Android to access virtual apps & desktops and Microsoft RDP based connections inside Accops container				x	x	x			x	x	x			
6	Accops Workspace client for iOS & Android to access native mobile apps & email client				x	x	x			x	x	x			
7	Reverse Proxy Gateway for clientless access to web applications					x	x				x	x			x
8	Clientless access to Windows & Linux PC/VM using RDP using HTML5 supported browser (HyLite)			x	x	x	x					x			
9	Seamless file transfer, endpoint security, USB redirection and other advanced features for Clientless portal using HTML5 browser			x		x	x					x			
K	Application Support for Remote Access														
1	Remote access to web application, SaaS apps					x	x			x	x	x			x
2	Remote access to Internal applications; client-server, RDP, SSH, any other client-server applications, VDI solutions					x	x			x	x	x			
3	Integrated Access to Virtual applications & Virtual Desktops : Accops HyWorks support				x	x	x			x	x	x			
4	Access to VOIP & other real time applications through UDP based tunnel for jitter free experience					x	x			x	x	x			
5	Access to MyDesktop: Office PC access, remote desktop and file share				x	x	x		x	x	x	x			
6	Self-service for password and account lockout management					x	x	x			x	x	x	x	x

	FEATURES	HyWorks Silver	HyWorks Gold	Virtual Browser	Digital Workspace Silver	Digital Workspace Gold	Digital Workspace Platinum	HyLabs	HyLite	HySecure Silver	HySecure Gold	HySecure Platinum	HyID Silver	HyID Gold	HyID Platinum
L	Authentication & Authorization for Remote Access														
1	User Authentication Support: Microsoft Active Directory, LDAP, Novell e-Directory, Local Database			x	x	x	x	x	x	x	x	x	x	x	x
2	User Authentication Support: RADIUS Server, SAML, ADFS, oAuth			x	x	x	x	x			x	x		x	x
3	SSO for web & SaaS apps using SAML, oAuth (IDP initiated authentication)					x	x				x	x		x	x
4	MFA using OTP tokens (SMS, Email), Mobile App token, hardware token					x	x	x	x		x	x	x	x	x
5	MFA using FIDO Security Keys					x	x	x	x			x		x	x
6	MFA using push notification to Desktops						x					x		x	x
7	MFA using push notification to Smart phones						x					x		x	x
8	Contextual login and app access based on device Identity				x	x	x	x	x	x	x	x	x	x	x
9	Contextual login and app access based on device location, health and more advanced parameters (Device classification service)											x		x	x
10	Contextual access to Virtual apps & desktops and apps within VDI based on device Identity (Device classification service)						x								
M	3rd Party Applications: Multi-Factor Authentication & SSO														
1	MFA connector for SAML supported apps (SP initiated auth) & ADFS												x	x	x
2	MFA connector with Apps supporting RADIUS (network devices, etc)												x	x	x
3	MFA connector with AD integrated apps using LDAP Proxy												x	x	x
4	MFA connector for Accops biometric server & 3rd party biometric (face & fingerprint) authentication server						x							x	x
5	Contextual MFA based on device ID, user ID, application accessed, location, time					x	x				x	x		x	x
6	Step up authentication based on context					x	x				x	x		x	x
N	Endpoint Management & Controls														
1	Centralized endpoint inventory and categorization for devices used for remote access	x	x		x	x	x	x		x	x	x			
2	Push firmware and client upgrades to endpoints	x	x	x	x	x	x	x		x	x	x			
3	Map end users to endpoint devices and provide device contextual access	x	x	x	x	x	x	x		x	x	x			
4	Remote control and helpdesk support from datacentre				x	x	x			x	x	x			
5	Restrict Internet control: Whitelist or blacklist URLs or completely block Internet				x	x	x				x	x			
6	Restrict local LAN access				x	x	x				x	x			
7	Restrict apps from downloading data, printing, drag & drop				x	x	x				x	x			
8	Restrict clipboard, print screen, screen recording, screen scrapping tool, screen sharing tool. Create exceptions for specific program and tools				x	x	x				x	x			
9	Restrict clipboard to work within specific application for better control				x	x	x				x	x			
10	Block USB port				x	x	x				x	x			
11	Run in stealth mode on end user PC with no option to stop the agent. Password protected install and uninstall				x	x	x			x	x	x			
12	Data copy protection on endpoint machine by blocking screen shot, clipboard, screen recorder blocking				x	x	x				x	x			
13	Announcements for users	x	x		x	x	x								
O	Management, Reporting & Compliance for Remote Access														
1	Centralized web-based management console with dashboards	x	x	x	x	x	x				x	x	x	x	x
2	Watermark for End-user PC					x	x				x	x			
3	Built-in load balancing of user traffic for virtual apps & desktops and other private applications: load balancing algo; resource utilization, application availability, round robin			x	x	x	x		x	x	x	x	x	x	x
4	Integration with Accops Reporting Server		x	x	x	x	x	x	x		x	x	x	x	x

P	Other Add-on solutions	Available as Independent SKU	Accops Workspace Platinum	HySecure Platinum	HyID Platinum
1	Accops Reporting Server	x	x	x	x
2	Accops Biometric Server: Fingerprint, Facial Auth	x			
3	Accops Enhanced USB Redirection Module	x	x		
4	Accops NanoOS to repurpose old PC, OS on USB	x	x		
5	Advanced Linux thin client management with complete firmware configuration including 3rd party components, monitoring and control (Needs additional thin client management software license)	x			
6	Accops HyMobile: Comprehensive Mobile device management for iOS and Android devices for company owned devices as well as personal (Needs additional Accops HyMobile MDM Solution License)	x			
7	Teradici PCoIP Cloud Access Plus license for heavy graphics applications (monthly or annual subscription)	x			

x: Feature available

x*: Feature available with add-on components

Blank or "-": Feature not available in this edition and needs upgrade to higher version

ACCOPS NANO OS

Features	
Accops customized Linux OS for PC refurbishing	✔
Kiosk Mode Operation	✔
Support for HySecure and HyWorks	✔
NO access to local disk	✔
Access to Virtual Desktops	✔
Access to Hosted Applications	✔
Secured OS (SCAP standards)	✔

ACCOPS SEP (Enhanced Driver)

Features	
Redirect USB devices to Microsoft RDS Server for Shared Hosted Desktops	✔
Redirect USB devices inside Windows 7, Windows 8 & Windows 10 based OS for Dedicated Virtual Desktops	✔
Redirect devices based on device type	✔
Redirect printers, scanners, biometric devices, USB security tokens, other USB devices	✔
Redirect Parallel (LPT) and Serial (COM) ports	✔
Concurrent User Licensing	✔

Note: The information contained in this document is subject to change. For the latest details, please refer to the commercial proposal document received or talk to an Accops authorized sales professional.



Accops, HyWorks, HyDesk, HyID, HyLite, HySecure and HyLabs are registered trademarks of Accops Systems Pvt. Ltd. Other names may be trademarks of their respective owners. Accops has the right to change, modify, transfer or otherwise revise the publication without notice.

Tel: India +91 96374 52253 | Email: sales@accops.com | Web: www.accops.com
Copyright © 2021, Accops Systems Pvt. Ltd. All Rights Reserved.