Embracing the Digital Workplace with Desktop Management Solutions

wanstor

Contents

wanstor

Introduction

Workers attitudes, habits and expectations are changing. They want to be able to work and have access to work any time; from any location; using whatever device, connection, and collection of apps happens to be most convenient.

This changing mindset has created a major shift in how business and not for profit organisations define the concept of a *"digital workspace"* and has forced IT teams to develop a new approach for delivering resources and information to their users.

In the past, a typical workspace was a defined area in an office building where people performed most of their work on a managed, company-owned PC and accessed all of their IT resources and applications over a carefully secured and maintained corporate network.

In this traditional environment, it was relatively easy for the IT team to make and enforce rules and strictly control access and compliance.

Even when users worked remotely, IT could still make the rules on how users connected to the network and what they were allowed to access. This kind of *"command and control"* approach to IT management is now very much a thing of the past.

Today, users think a workspace is anyplace they have access to a wired or wireless Internet connection and a corporate owned or personally enabled desktop, laptop, smartphone, or tablet.

To make matters even more complicated, today's users expect a responsive, flexible experience every time they interact with technology.

They are used to discovering their own technology solutions, whether it's downloading an app from an app store, finding and using a cloud-based service (public or private), or having access to the nearest public Wi-Fi network to stay connected, or Googling answers to their computer issues.

If their company IT department is unable to deliver the types of flexible, functional experiences they expect, users (more so than ever before) will simply take matters into their own hands, which creates obvious and unacceptable risks.

So the key question facing IT Managers today is *"How can your organisation provide the kind of "any location, any device, any service, any connection"* workplace your users want. All the while not compromising the IT' teams ability to keep the user and the wider organisation secure and compliant?"

wanstor

Meeting today's elevated self service expectations

At Wanstor we believe the answer requires a fundamental shift in the relationship between IT teams and the workers they support; from a rigid, *"command and control,"* device-centred management mindset to a user-focused approach that works to provide safe, appropriate access to any workspace on any device in any location.

The right desktop management solution should embrace and enable this kind of user-centric, digital workspace experience by extending several key capabilities to any user, device, and wired or wireless connection. For example:

- **User Self Service:** Allow users to access the apps, resources, information, and support they need quickly and easily, so they do not need to take matters into their own hands and work around IT
- **Automation capabilities:** Enable IT teams to manage the increasingly complex mix of users, devices, applications, and information in their organisation with less time and with less effort
- **Single view management:** Consolidate all desktop management capabilities and functions into a single management console

This will give IT Managers a complete, integrated, and uniquely user centric view of their diverse corporate workspaces. It will also make it easier to deliver IT services and resources quickly and efficiently.

The right desktop management solution will also provide security that extends far beyond the boundaries of the corporate environment to give users appropriate, location aware access to apps and information from any device over any connection.

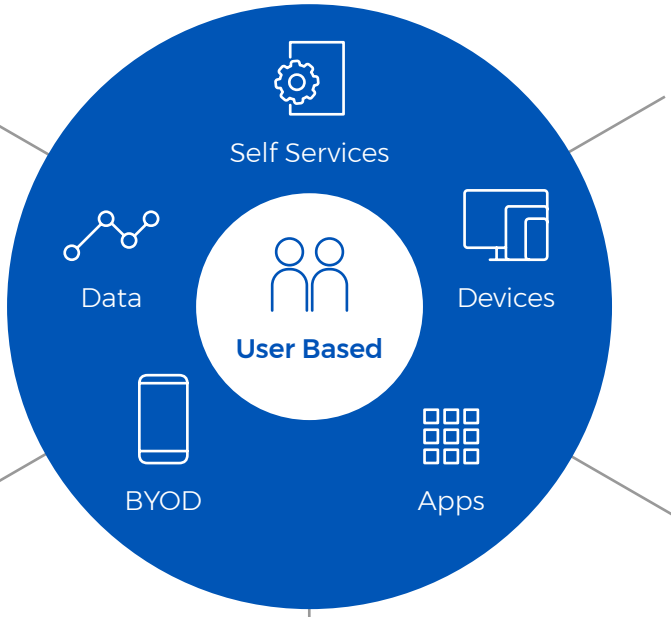
It should also contain compliance solutions for traditional desktops and laptops, mobile devices, and applications that never force users to choose between flexible remote access and the compliance requirements of the organisation they are working for.

In the rest of this document Wanstor's Desktop Management experts provide a more detailed guide for what to look for in a desktop management solution that can really enable a business or not for profit organisation.

The framework of the modern, user-focused workspace

User Self Services

Request, track, activate, print, file share and much more from the workspace



Automation

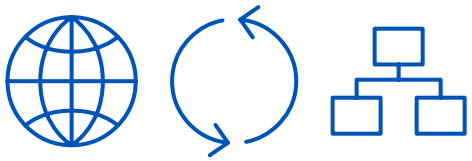
Workspace automation process for all devices and self-services by selecting any services from any device

Compliance

Assure workspace compliance for your assets, licenses, apps, devices and contracts

Security

Secure the workspace through endpoint security, encryption, location awarreness, wireless security and containerisation



Single Pane of Glass

Seamless integration of all IT systems by providing a complete view of the workspace

wanstor

In today's modern working environment the term *"self –service"* has evolved. Self-service is about much more than allowing users to reset their own passwords. It's about giving them a complete set of tools to solve problems and gain access to new apps and information quickly; from any device or location.

Allowing users access to a complete collection of self-service tools reduces the strain on the IT department. It also removes the motivation for users to look for answers and resources from outside, unsecured, and non-compliant sources.

IT Service Management (ITSM) should give users direct, convenient access to a complete catalogue of service options from any device. At Wanstor we suggest IT Managers offer their users a convenient app to create their own service ticket, track the progress of the incident, and interact with the helpdesk team; all without ever having to place a call.

This saves the user and the service desk time and effort in resolving questions and queries as all the information is readily available to both helpdesk agent and end user.

A service catalogue also allows IT teams to create a convenient, familiar online store experience where users can request new IT resources including hardware, software, and any other assets made available in the catalogue. This makes every interaction with the IT team as easy as possible. Additionally it makes every part of the helpdesk operation more efficient and effective.

BYOD Made Easy with Mobile Management

How many people in your business or not for profit organisation already rely on their smartphones as much or more than their office PCs?

IT teams often recognize and embrace this mobile reality, and mobile management makes it possible to turn any mobile device into a secure, managed, and effective business tool.

Effective mobile management should provide users with the capabilities they need to keep their mobile devices (and the corporate information on them) safe and protected.

This starts with the ability to track, lock down, or wipe their mobile device if it gets lost or stolen. Mobile management should also allow IT teams to create a separate secure and managed container for business apps and information on personal devices.

This capability gives users an easy, convenient way to access and use corporate apps and information on their own smartphones or tablets.

It also keeps business and personal apps and information separate, and it puts a crucial extra layer of management and security around the corporate resources and information the IT team needs to protect.

Access Containerized Apps Quickly and Easily

Finally, creating desktop containers makes it easy for users to find, install, and use applications on their desktop and laptop PCs.

With the right desktop containerization offering, users can visit a portal that looks and feels like an online store, select the apps they need, and start using them in a matter of minutes on any machine.

> **Users should have the option to stream these virtualized apps live if they don't want to take the time to download them**

Together, these capabilities allow IT teams to give users the kind of easy, convenient, and complete self-service experiences they want and expect, which helps IT departments strengthen their reputation as a relevant, service oriented operation.

The other major benefit is effective self-service releases IT resources, so key members of the IT team can focus on more important, strategic projects.

Automate Your Workspace Environment

With increasing user expectations, the number and variety of mobile devices and cloud services increasing, and the breakdown of the boundaries between work and personal time, it is probably an understatement to say that the IT environments that support modern workspaces are growing more diverse and complex.

> In the face of this complexity, more sophisticated levels of automation become essential

Without automation, complexity quickly turns into chaos. An effective Desktop Management solution addressing this challenging dynamic will have built-in advanced automation capabilities.

These capabilities should include the ability to automatically image new devices, deploy patches, package and distribute apps, remotely encrypt devices, and more.

A good desktop management solution should also make it possible for users to select and automatically launch a variety of services from any device they happen to be using, without any direct involvement from IT.

One single view of the workspace

Desktop Management should be more than a family of loosely connected endpoint management and security products. Instead, it needs to be a tightly integrated set of tools that work together to simplify, streamline, and automate every part of your workspace infrastructure.

Desktop Management should include a centralised management console that provides a true single view for performing all of your security, patching, containerization, self-service and device management tasks, so the IT team can eliminate the inefficiencies of multiple disconnected tools.

This console should make it possible for IT Managers to embrace a smart, user-centric approach that shifts the focus from managing individual devices to providing users with the tools they need to be productive in any workspace based on their roles and identities.

In practical terms, this will save IT teams the time and hassle of managing every individual device in their organisation, especially when users carry multiple devices or move from location to location.

Finally, the management console should feature a robust collection of system dashboards, workflows, hot lists, and other tools that make integrated, unified workspace management a reality.

More user freedom through improved security

Every IT team wrestles with the tension between providing users with the easy, flexible access they want; and keeping information and assets secure and compliant.

The right desktop management solution should help resolve this tension through sophisticated security capabilities, so IT teams can expand access to resources, apps, and information beyond the walls of their organisation without putting the business or not for profit organisation at risk. This should include:

- Complete, automated patch management that monitors patch compliance on all Windows and Linux endpoints, quickly identifies and assesses vulnerabilities, and applies updates to keep all your endpoints patched and secure.
- Full disk encryption that protects every bit, byte, and file on every PC in the organisation, so IT teams can stop worrying about security breaches and data loss.
- Policy-based data encryption that creates “safe harbour” encrypted folders on PCs and fully encrypts removable storage devices.
- Wi-Fi management and security controls that allow IT teams to create white and black lists for wireless access points, enforce policies that restrict or block Wi-Fi communications based on set security or encryption standards, and more.
- USB and storage device security that allows IT teams to enable, disable, and set access rights for removable storage devices, provides granular white listing controls for USB devices, prevents unauditable transactions on local storage devices, and more.
- Advanced firewall protection that provides Network Driver Interface Specification (NDIS) level security for network traffic the moment it enters a company PC.
- Policy-based application control that blocks known malicious applications, controls access to applications based on a user’s location, and makes sure that the proper security applications are running on endpoints.
- A complete mobile security solution that enforces password usage and encryption on mobile devices, makes it easy for users to remote wipe or disable lost or stolen devices, provides detailed security reporting, and more.
- A secure desktop containerization solution that packages all of the files, settings, runtimes, and components applications need to run in one secure and protected container.
- Mobile application management that provides IT teams with the ability to manage enterprise apps and data on an end-user device, without compromising end-user privacy.

With the right desktop management solution, all of these security capabilities should work together to help IT teams extend the boundaries of their security perimeter, grant appropriate safe access to any device, and ultimately keep users and information safe in any workspace environment—whether it's a wired PC in a cubicle at your corporate headquarters or a tablet accessing a public Wi-Fi connection at the airport.

Making sure compliance is front of mind

Compliance can quickly become a major challenge to IT Teams as they work to support the ever-expanding variety of devices, apps, locations, and connections that make up today's workspaces.

As IT environments inevitably become more diverse and complex (as users become more sophisticated and independent) tracking, enforcing, and documenting compliance can start to feel like an overwhelming task.

Desktop management from Wanstor approaches workspace compliance in much the same way it approaches workspace security; with built-in key features and capabilities.

This creates a complete, integrated compliance framework that is capable of accommodating and supporting all of today's workspace environments. Compliance starts with a proven asset management foundation for all traditional endpoints.

With some of the industry's most advanced asset discovery, inventory, auto license reconciliation, license compliance, and reporting capabilities, software asset management (SAM) should give you everything the IT Manager needs to eliminate license over- and under-purchasing, avoid costly licensing penalties, and comply with license agreements and regulations.

Next, endpoint security management, full disk encryption, and patch management should include the sophisticated tracking, enforcement, and reporting capabilities needed to maintain and prove corporate security and patch compliance across all organisational endpoints.

Finally, mobile management extends these asset and security tracking and management capabilities to all mobile devices; including both corporate and privately owned devices.

With mobile management, IT Managers should be able to accurately track licensing and usage on any mobile device, so they can always know and document what you have, what's being used, and how many are needed paying for no matter how many different apps or BYOD devices the IT team are dealing with.

Together, these compliance capabilities make sure the IT Team always have the tracking, enforcement, analysis, and remediation tools needed to keep all of workspaces compliant.

Start Enabling Your Secure, Compliant, and User-Centric Workspaces Today

As modern workspaces continue to evolve, a few things are clear. Workers will continue to become even more dependent on an even wider range of mobile devices.

The boundaries between work and personal will continue to disappear

The expectations of being able to get work done from any location, using any device or service, over any wired or wireless connection will continue to grow.

To succeed and thrive in this reality, IT teams need better, more aggressive tools that support and enable today's diverse workspaces.

Desktop management should embrace this challenge, with solutions that extend the exceptional experiences and access users want, and the security, compliance, and control businesses require, to any workspace environment.

wanstor

ManageEngine Desktop Central Overview

To help business and not for profit organisations manage their IT estates, Wanstor has partnered with ManageEngine to design, deploy and manage their Desktop Central solution for customers in the UK.

Integrated Desktop & Mobile Device Management Software

Desktop Central is a unified endpoint management solution that helps IT teams manage servers, laptops, desktops, smartphones, and tablets from a central location.

By using a Desktop Central solution from ManageEngine, IT teams can automate regular desktop management routines like installing patches, distributing software, imaging and deploying OS, managing IT Assets, managing software licenses, monitoring software usage statistics, managing USB device usage, taking control of remote desktops, and more.

It supports managing Windows, Mac and Linux operating systems. It also helps IT teams to manage mobile devices to deploy profiles and policies, configure devices for Wi-Fi, VPN, email accounts and so on., apply restrictions on using cameras, browsers and so on, and to secure devices by enabling passcode, remote lock or wipe. IT teams can manage all iOS, Android and Windows smartphones and tablets using one tool.

The need for unified endpoint management

IT asset footprints are growing rapidly in today's business and not for profit organisations. Managing these assets has become more challenging for IT teams with the ever-increasing numbers of laptops, desktops, tablets, and mobile phones, which are otherwise known as endpoints.

The best way for IT teams to make sure devices are being managed properly is by employing endpoint management software. Endpoint management becomes even harder with varied devices, or with devices that travel outside of the organisation's network.

wanstor

Benefits of unified endpoint management

Single-solution architecture	A single, centralised platform for endpoint management will help IT teams avoid complicated integrations among different software on multiple platforms. They will no longer need to compile, compare, and evaluate reports from different sources.
Ease of onboarding	A unified endpoint management platform allows organisations to easily push out device policies, applications, and environments, meaning devices go from out-of-the-box to in-use faster and with better baselining.
Helps improve IT security	Security is one of the primary concerns for any organisation today. Recent ransomware attacks just prove how dangerous zero-day vulnerabilities can be. A unified endpoint management solution makes it easy for IT admins to keep track of suspicious activities across all endpoints.
Improved visibility	Enterprises can monitor inventory, usage, vulnerable systems, and much more from one place. This visibility provides not only opportunities for cost saving, but also the ability to troubleshoot, diagnose, and resolve issues remotely.
Unified corporate IT environment	All the benefits of a unified endpoint management platform combine to deliver the single greatest advantage to organisations: a unified corporate environment in which experience is optimised across the organisation on corporate networks.

What is unified endpoint management?

Unified endpoint management is an umbrella approach to managing all the endpoint devices within an organisation from a central location.

In general, a typical unified endpoint management solution provides secure updates, patch management, automatic hardware and software inventory tracking, logging, mobile device management, software and OS deployment, workstation remote control options, license management, and overall quick remediation capabilities for IT professionals.

wanstor

Key Desktop Central Features: Desktop Management

Desktop Management
Manage Windows, Mac and Linux

Patch Management
Automate patch deployment per OS and other third party applications, shield Windows and Mac from security threats

Asset Management
Manage your IT assets, Software Metering, Software License Management, Prohibited Software, and more

Active Directory Reports
100+ out-the-box reports provides a quick and complete insight of the Active Directory infrastructure

USB Device Management
Restrict and control the usage of USB Devices in the network both at the user-level and at the computer-level

Remote Control
Troubleshoot remote desktops with multi-user collaboration, file transfer, video recording, and more

Service Pack Installation
Scan and detect missing service packs of OS and Applications and automate deployment to stay up-to-date

Software Deployment
Simplify software distribution to install and uninstall software with built-in templates for package creation

Windows Configurations
25+ predefined configurations including Power Management, USB Device Management & Security Policies

User Administration
Define roles with selective privilege and delegate users to these roles for effective management

Power Management
Apply energy saving power schemes, shut down inactive computers and get system uptime reports

OS Deployment
Comprehensive disk imaging / deployment feature supports deployment needs in both offline and online mode

Mobile App
Start managing your desktops and servers on the go. Download mobile app for iOS devices

Key Desktop Central Features: Mobile Management

Mobile Device Management
Manage iOS, Android and Windows

Device Enrollment
Enroll devices manually, in bulk or let users self-enroll their iOS or Android devices with two factor authentication

Asset Management
Scan to fetch details of installed apps, enforced restrictions, installed certificates and device hardware details

App Management
Distribute in-house and store apps to devices, remove or disable blacklisted apps, assign redemption codes for commercial apps and more

Security Management
Configure stringent security policies such as passcode, device lock to protect corporate data from outside threats.

Profile Management
Create, configure and associate policies and profiles for different departments, roles or groups

Audit and Reports
Audit mobile devices with out-of-the-box reports such as Rooted Devices, Devices with Blacklist Apps, etc.

In-depth focus: Asset Management

An IT administrator must be up-to-date on the information about the software and hardware used across the organisation they work for. Manual compilation and reconciliation of IT assets is effort-intensive and error-prone.

Desktop Central's web-based inventory management not only helps automate this task, but also provides out-of-the-box network inventory reports.

Inventory management features

- Perceive audit ready hardware and software inventory details.
- Schedule scanning of systems to collect inventory data.
- Manage software licenses, category, and compliance.
- Detect, block, and auto-uninstall prohibited software in the network.
- Have real time access to software usage statistics.
- Automate alerts on specific events such as installation or uninstallation of new software, removal of hardware, etc.
- Over 20+ out-of-the-box reports and the ability to create custom reports across different formats.

Scheduled inventory scanning

Desktop Central scans the Windows desktops and servers in the network periodically to collect hardware and software details and stores them in your the database. The inventory scanning interval is flexible and can be configured to meet the real-time needs of your organisation. This enables administrators to have access to up-to-date inventory information any time, without any manual intervention.

Alert notifications

Desktop Central sends email notifications to IT administrators for the following events:

- New hardware is added or removed in the network
- New software is installed or uninstalled in the network
- Non-compliance of software licensing policy
- Prohibited software is detected in the network

Hardware inventory

The hardware inventory provides complete details about the hardware used in the network. The hardware inventory reports helps IT administrators to:

- Sort computers by memory
- Sort computers by OS and service pack version
- Sort based on hardware manufacturers
- Sort by age, disk usage, type

Software inventory

Software inventory in Desktop Central gives IT Administrators access to:

- **Software metering:** Usage details of specific software such as number of times it has been used, total usage duration, systems with specific software etc.
- **Software details:** View commercial and non-commercial software information including vendor name, installation date, and software version.
- **Software license compliance:** Provides the ability to view the compliant and non-compliant software being used in the network.
- **Prohibited software:** Blacklist software, block executables through, and auto-uninstall prohibited software in the network.
- **Warranty management:** Track the warranty information of the hardware assets managed by your IT team.

Network inventory reports

Desktop Central provides out-of-the-box reports to view the software and hardware details of the network. These reports help IT administrators to gain a quick and accurate view of the network inventory.

The ability to export reports to PDF or CSV formats help integrate with third-party reporting engines or to print it out for future reference.

Achieving ROI from your Desktop Central Investment

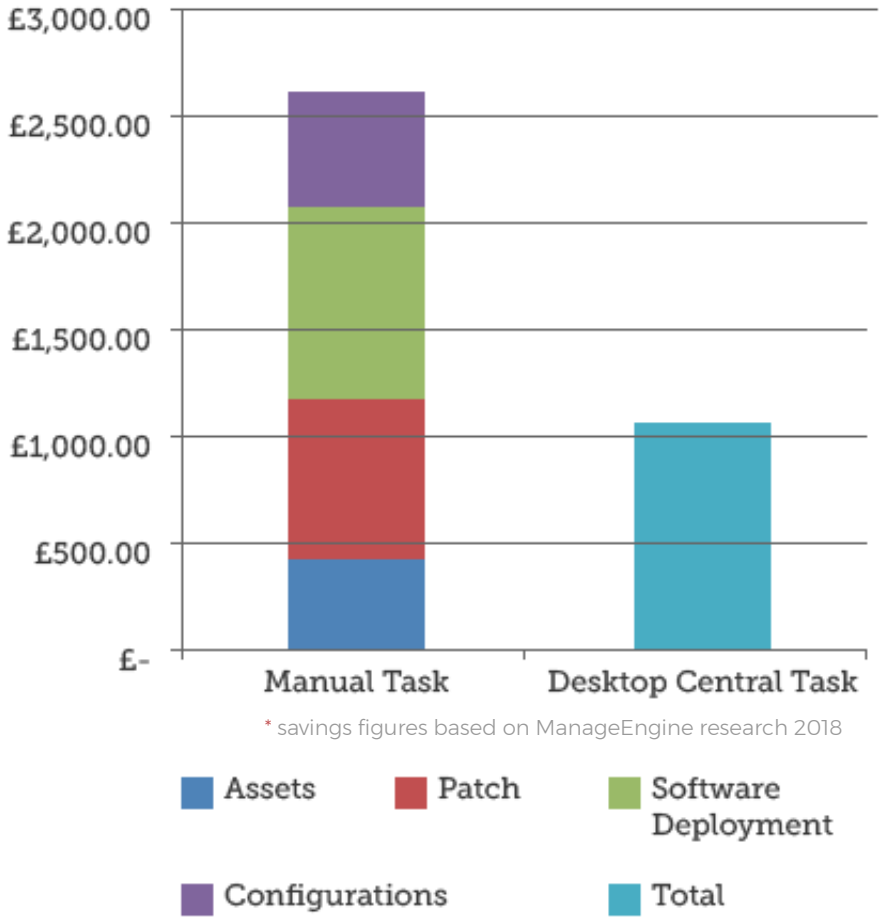
This example will demonstrate how Desktop Central saves IT teams, time, money and effort with a relevant and robust ROI calculation

Assumptions

Network of 100 computers
Hourly salary for a technician is £35

Notes

- While the cost of executing each task manually can be calculated, this is difficult within Desktop Central as it is integrated software. The graph to the right shows the total cost of performing these tasks using Desktop Central as opposed to manually.
- Whether IT teams do these tasks once or multiple times a year, the cost of doing it with Desktop Central is going to remain the same or may increase marginally, if you take into account the time spent by the technician in initiating the tasks from the management console



* savings figures based on ManageEngine research 2018

Manual task execution vs Desktop Central task execution

Task	Manual Execution		Desktop Central Execution		Annual Savings
	Man-Hours	Cost	Man-Hours	Cost*	
Performing asset scanning, patch management, software deployment, and configurations once in a year	114	£3,990	2.63	£1,087	**£2,903**
Perform Asset scanning once in a quarter, install patches once a month (excluding Microsoft Patches), install software and configure systems once a year	284.92	£9,972	2.63	£1,087	**£8,885**
Perform Asset scanning once in a quarter, install patches once a month (excluding Microsoft Patches), install software and configure systems once a year	484.84	£16,969	2.63	£1,087	**£15,882**

* includes an additional £995 towards the annual subscription fee for 100 computers

Comparing Manual task execution vs Desktop Central task execution

Procedure	Time per Computer	Time per 100 Computers (Manual)	Time per 100 Computers (Desktop Central)
Manual Scan to get hardware and software details	5 Mins	8.33 Hours	**2 Mins**
Identify missing patches for 3rd party applications like Adobe, Java, Firefox, etc.	3 Mins	5 Hours	**2 Mins**
Download required patches from the vendor's website and install them	5 Mins	8.33 Hours	**5 Mins**
Identifying missing Microsoft Patches	5 Mins	8.33 Hours	**2 Mins**
Downloading and Installing missing Microsoft Patches	5 Mins	8.33 Hours	**5 Mins**
Deploying simple software app	3 to 5 Mins	5 to 8.33 Hours	**2 Mins**
Deploying MS office applications	15 Mins	25 hours	**15 Mins**
Installing Service Packs	3 Mins	5 Hours	**2 Mins**
Configuring display settings, application settings, browser settings	3 Mins	5 Hours	**2 Mins**
Applying security policies, restricting USB device access, file restrictions	5 Mins	8.33 Hours	**5 Mins**
Local user management, mapping drives, installing printers	5 Mins	8.33 Hours	**5 Mins**

10 Reasons your IT team needs to purchase Desktop Central today

Integrated Desktop and Mobile Device Management Solution	▪ No need to rely on multiple tools for managing Desktops and Mobile Devices ▪ A single management console for all desktop and Mobile management tasks
Enhances Network Security	▪ Helps patch systems and applications automatically ▪ Enables administrators to apply windows security policies ▪ Restricts and customizes external device usages like USB, external hard disk, etc. in enhancing network security
Increases Productivity	▪ Robust support for BYOD ▪ Fosters collaboration between employees with their mobile devices ▪ Enables employees to access corporate resources from anywhere
Manages Distributed Environment	▪ Manages geographically distributed computers, devices and users from a central management console ▪ Allows setting up distribution points to minimize the WAN bandwidth consumption ▪ Provides control on mobile devices irrespective of location
Higher Return of Investment (ROI)	▪ Saves operational costs by automating various routine activities like Patch Management, Software Deployment, mobile application ▪ Manages BYOD and save costs from investing in new devices ▪ Enable and set up Power Management to see immediate savings on desktop power consumption ▪ Effective software license management will save cost of unused licenses ▪ Accessing asset information, installing software, tracking tickets now performed within single console i.e. by integrating Desktop Central with Service Desk Plus
Reduces Training Costs	▪ Simple point and click installation package includes an embedded relational database and webserver ▪ Saves working with multiple packages reducing training costs by providing a simple, user-friendly interface
Completely Web-based	▪ Completely web-based offering unparalleled flexibility in accessing the systems and mobile devices from anywhere
Integration with other ManageEngine Products	▪ Seamless integration of data with ManageEngine ServiceDesk Plus and AssetExplorer ▪ Help Desk and Desktop Management functions can be performed from single integrated console ▪ Integrates with ManageEngine Products such as Servicedesk Plus and IT 360 Applications
Easy Installation & Setup	▪ Single installation package including all required installables such as database and web-server ▪ Installation within 10 minutes and setup within one hour
Affordable Solution	▪ Offers competitive price and ease of deployment on standard hardware, supporting desktops, mobile devices and servers ▪ Accustoms without steep learning curve

Wanstor Customers using ManageEngine Desktop Central

Final Thoughts

Today's modern worker is no longer confined to a physical office or a Windows desktop or laptop. Although traditional Client Management Tools (CMT) would have been sufficient in the past, they are no longer enough to manage the increasing diversity of platforms and devices, BYOD, and frequent Windows 10 updates.

While many business and not for profit organisations have adopted Enterprise Mobility Management (EMM) solutions to manage mobile endpoints, maintaining both CMT and EMM without any integration is highly inefficient. Instead, IT teams need to select the right Unified Endpoint Management (UEM) solution.

Unified Endpoint Management combines traditional Client Management with Enterprise Mobility Management providing the IT team with a single view to manage devices, apps and data.

For more information about Wanstor and ManageEngine's Desktop Central solution please email us at **info@wanstor.com** call us on **0333 123 0360** or visit us at **www.wanstor.com/manageengine-it-management-software.htm**

Wanstor | 124-126 Borough High Street | London | SE1 1LB |

info@wanstor.com

© Wanstor. All Rights Reserved.