Scalefusion for Windows Device Management

Manage Windows based computers, laptops, and point-of-sale systems with ease. Push necessary apps and content, patch updates, and take remote control of your Windows endpoints and make them work for your business.

Overview

Manage legacy and modern Windows devices in an enterprise environment. Push business-specific applications, security policies, and configurations to heighten employee productivity on Windows devices.

Benefits

- Drive faster device enrollment
- Manage all your Legacy and Modern Windows Devices (Windows 7, 8.1 & 10, 11)
- Push OS and Third-Party App Updates remotely
- Run the device in single or multi-app kiosk mode
- Drive application management for public and enterprise apps
- Drive enhanced security for corporate data
- Push relevant business content with ease
- Quickly resolve device issues with Unattended Remote Cast and Control

Introduction

Scalefusion MDM empowers enterprise IT teams to configure and manage Windows laptops and computers for their businesses. With the Scalefusion dashboard, IT administrators can create diverse policy configurations and push them onto the devices over the air.

With Scalefusion, monitoring a large inventory of both legacy and modern Windows devices (Windows 7, 8.1 and 10 , 11) is streamlined. IT admins can create a team-wide or enterprise-wide application usage policies to keep devices and applications up-to-date with automated patch management. Scalefusion aids the IT teams in provisioning the Windows devices with security settings, network configurations, and business resources to ensure that employees can start working instantaneously.

Windows: The Chosen One

End-users- be they employees or customers, who deal with digital devices for business enjoy familiarity. Windows holds more than 80% of the market share in desktop operating systems, which makes it evident that Windows is a popular choice over the rest. Microsoft released the first version of Windows in the mid-1980s and has continued to upgrade it since then. When Microsoft launched Modern Windows, it took “mobile-leaning” user behavior into consideration and incorporated a light-weight, clutter-free and seamless user experience specially designed to suit Gen Z users. More and more advancements were made, making the Windows devices as sleek and as mobile, as a mobile phone.

Naturally, as Windows upgraded from a PC-centric operating system to a device-agnostic operating system, managing Windows devices in enterprises have become a key concern for enterprise IT admins.

While managing Windows devices for enterprises, it is critical to ensure that corporate data on the devices is secure at all times, the device can be equipped with business resources, and the enterprise IT team can minimize distractions, making

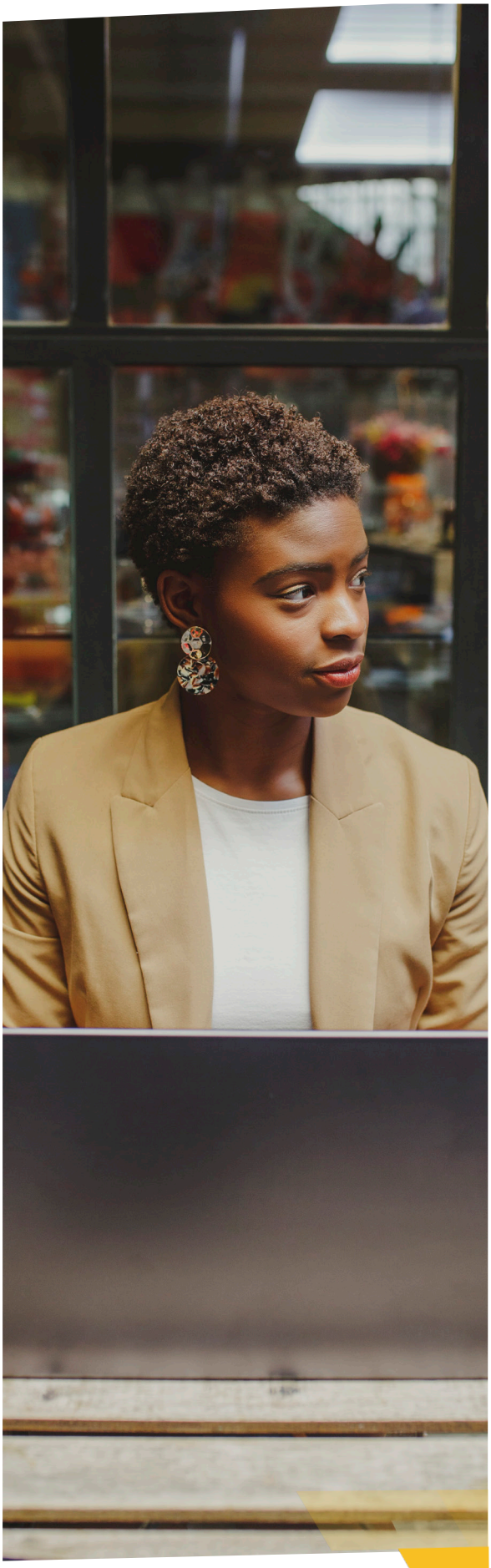
them packed full of elements boosting employee productivity. On the other hand, when Windows devices are deployed as customer-facing kiosks or POS systems, the IT teams have to ensure a seamless end-user experience across the entire device inventory.

And this is why enterprise IT teams have to make a focus-shift from conventional PC management to a comprehensive Windows Device Management.

Scalefusion for Windows Device Management

Windows device management has never been straightforward, and IT teams often struggle to strike the right balance between management and excessive control hampering device usability. Hence, onboarding an MDM solution that offers an effective and easy way to manage the Windows devices is the right choice to make.

Primarily, Windows device management should focus on solving the most critical and urgent IT needs - from easy enrollment to application delivery and security management to reporting. Scalefusion MDM for Windows goes above and beyond the basic capabilities of an MDM and presents a centralized management console to ease the task for enterprise IT admins.



Manage your Legacy & Modern Windows Devices

Gain granular controls and take your device management to the next level. Set Windows 7, 8.1 & Windows 10,11 devices in motion without hampering the user experience. Configure your devices to run in single or multi-app kiosk mode with the Scalefusion MDM agent.

Policy Configuration, Utility Configuration and Updates

- **Utility Configuration**

Once the Windows devices are enrolled in the Scalefusion MDM, they run a default policy configuration or a specially created device profile configuration. This configuration is highly customizable and can be created, updated, and reflected on the device inventory at any time.

This configuration includes:

• Pushing secure Wi-Fi network configurations allowing employees to plug and work in multiple office premises.
• Reflecting the organization branding on the device inventory
• Pushing Exchange Active Sync or POP/IMAP settings on the devices.

- **MDM Agent**

The Windows MDM agent is an app developed by Scalefusion to enable IT teams to leverage capabilities that are not available within the Windows CSP. Using the Windows MDM agent, IT admins can push and execute Powershell scripts from the Scalefusion dashboard on managed Windows devices. These scripts can be used for automating processes such as adding network drives, installing applications, pushing security software updates, and granting new users access to shared files on managed Windows devices. The agent can also be used to put the devices into single or multi-app kiosk mode, especially for versions where the kiosk mode feature has been deprecated when modern management was introduced .

The MDM agent can also be used for advanced reporting for:

User Information: Last logged in and current logged in user details

User Activity: The number of users accessing the device, the most active users and activity statistics

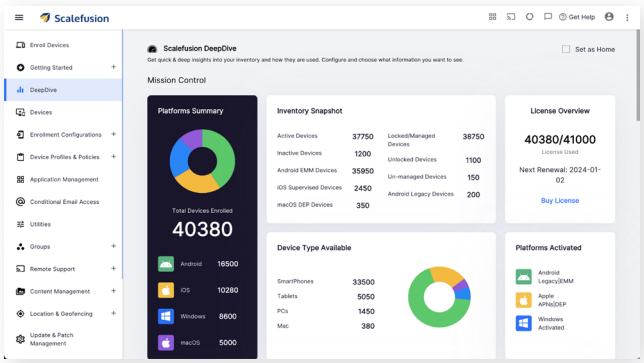
- **Custom Settings**

Scalefusion provides IT admins an option to create their own CSPs and push it to the managed Windows devices via Scalefusion dashboard. By using the Custom Settings feature of a Scalefusion Windows Profile, IT Admins can use a top-notch XML editor and push a CSP directly to the devices.

Easy Enrollment

With Scalefusion, IT teams can choose to enroll and provision individual Windows devices with management policies or choose to automate it with the help of the Windows Autopilot program for an OOBE (out-of-box-experience). Scalefusion has now streamlined its authentication process for managed devices into one that provides faster and more reliable security for its end users. With the configuration of SAML, Scalefusion allows IT admins to access the dashboard using SSO (single sign-on) using Okta, Office 365 AD, G Suite, or PingOne IdP.

This essentially saves manual IT time in configuring the devices individually, while also ensuring that employees can begin using the device by connecting to the nearest network and entering their Azure AD credentials.



Patch Management

Scalefusion helps you keep your Windows devices updated with the latest OS and Third-Party Application Patches. Identify Windows OS patches that can address security vulnerabilities and apply them remotely. Check for available application updates and push them automatically. Simplify security and compliance by ensuring that your Windows devices and applications run on the latest versions at all times.

Single App/Multi-App Kiosk Mode

So far, we've discussed the settings available within Scalefusion MDM when Windows devices are used by employees. But one of the other popular use-cases of Windows devices is as kiosks. These kiosks can be deployed as wayfinders in public places, as a part of the POS system, or as a public browser. To ensure the security and business usability of Windows kiosks, Scalefusion MDM offers a single app or a multi app kiosk mode.

Application Delivery

One of the prime reasons why IT teams want to manage Windows devices in the enterprise environment is to deliver apps that help the employees accomplish their work quickly. With Scalefusion MDM, application delivery on managed devices is streamlined. IT admins can push the UWP app and Win32 apps via the Windows Business Store on the managed devices at the time of enrollment as well as later at any time during the device lifecycle. IT admins can also install private line of business apps on managed devices, including UWP and MSI apps.

- **Windows App Catalog**

Discover, install and update the latest versions of third-party apps right from the Scalefusion dashboard without need a need to connect your Scalefusion account to Windows Business Store with Windows App Catalog powered by Winget.

Make apps readily available for installation and configuration by adding them to to Windows App Catalog, also choose to auto update apps form the Windows App Catalog.

Conditional Email Access

Scalefusion offers Conditional Email Access to enable organizations to protect their company data and prevent unauthorized access to business emails. With this policy, IT admins can monitor managed devices that connect to an organization's corporate email server. Scalefusion CEA is user-friendly and flexible. It enables IT admins to set a grace period during which end users can enroll their devices in Scalefusion. If an end-user fails to comply with the Scalefusion enrollment policy even after the grace period has expired, access to the mailbox from the non-compliant device is denied in order to protect corporate email data.

Application Whitelisting and Blacklisting

Downloading unidentified apps on devices can serve as an invitation for malware, posing a serious threat to device and data security. To avoid such scenarios, IT admins can whitelist only select apps and block the end-user/employee from further downloading any application on the device. Alternatively, to ensure employee productivity, IT admins can take the application blacklisting route, where access to certain apps is blocked on managed devices using Scalefusion. Either way proves ideal to curb security challenges as well as distractions.

Browser Configuration

Scalefusion MDM offers configuration settings for the Google Chrome and Microsoft Edge browsers. IT admins can customize the startup settings, bookmarks, cookie policies, and other privacy settings on both of these browsers. Secure browsers by configuring browsing history, geolocation and incognito mode.

Website Whitelisting & Blacklisting

With Scalefusion MDM, IT teams can ensure secure browsing on the entire Windows device inventory, be it deployed as a kiosk or as a device for employees. Within the Google Chrome or Microsoft Edge browser, IT teams can populate a list of allowed or blocked websites. This not only helps in reducing distractions at work but also enables safe browsing, mitigating the threat from malware attacks on untrusted websites.

Content Management

For employees working remotely, streamlined access to business documents is critical. Similarly, Windows devices are deployed as digital signage kiosks where the content needs to be frequently updated remotely. Scalefusion enables remote content management where IT admins can push documents, image files, videos, and interactive presentations.

Extensive Security Configuration

After covering for security vulnerabilities that arise from accessing unknown websites and apps, IT teams can further secure the enterprise Windows devices with Scalefusion MDM's extensive security configuration. First things first, the IT teams can create a password policy, define the ideal password type, complexity, define a period after which it needs to be changed, and enforce it on the device inventory. Further, IT can configure Cortana and device peripherals like cameras, USBs, and Bluetooth.
Here's a list of security features available for Windows devices managed with Scalefusion:

- **Windows BitLocker**

To encrypt the device hard drive and protect the data when the device is offline, Scalefusion also enables the configuration of Windows BitLocker settings- a full volume encryption feature by Microsoft. Scalefusion enables IT admins to configure the BitLocker settings to help protect corporate data and to ensure that a computer has not been tampered with while the system was offline.

- **VPN Configuration**

Securing network access and ensuring corporate data security on devices working outside the corporate network perimeter are essential. With Scalefusion, IT admins can configure a VPN provider (native or third party) for managed Windows devices and route the traffic to the corporate apps and data via a secure network. IT administrators can also selectively enforce per-app VPNs.

- **Windows Hello**

Scalefusion supports Windows Hello for Business. IT admins can integrate Windows Hello for Business (formerly Microsoft Passport for Work) with Scalefusion. Using this integration, IT admins can enable Windows Hello based access and add an extra layer of security to the managed Windows devices.

End-users can use user gestures such as PIN or biometric authentication like a fingerprint or facial recognition to sign in to their managed Windows devices instead of a password.

- **Windows Defender Policies**

IT admins can add an extra layer of protection to managed Windows devices with Microsoft's Windows Defender, now known as Microsoft Defender Antivirus. Configure Windows Defender policies on Scalefusion and extend real-time protection against malware threats. You can configure policies such as scanning, real-time monitoring, signature updates, and cloud protection directly from the Scalefusion dashboard.

- **Certificate Management**

With Scalefusion MDM, you can enhance the deployment experience of Digital Certificates on devices, as well as provide enterprises additional features and benefits of implementing security across devices. Using the Certificate Management feature, IT admins can streamline the process of deploying digital certificates to end-user devices by automatically provisioning digital identities onto devices without end-user interaction. IT admins can also push digital identity certificates for authenticating enterprise Wi-Fi configurations on managed Windows devices via a certificate payload.

- **Lost Mode**

Lost mode allows IT administrators to mark a device as lost, locking it for all users and displaying a customized message, footnote, and phone number. Preventing unauthorized access and facilitating device recovery, enhancing organizations' device management strategy and data security.

UEM-integrated identity and access management

Bring the power of UEM and IAM to your business to enhance enterprise security and compliance. Simplify user identity and access management with Scalefusion OneIdP. Integrate your existing directory or create your own on the .oneidp domain. Authenticate users and authorize access to enterprise devices, data, and applications seamlessly. Ensure robust identity governance with single sign-on (SSO) to enable your employees to access work apps with a single set of credentials. Efficiently manage user lifecycles and extend access permissions based on device management status. Set access conditions for trusted locations, Wi-Fi networks, and IP addresses and deny access to work apps and devices via unidentified networks and locations.

Remote Troubleshooting

To reduce device downtime on managed devices, IT admins can make use of the Remote Cast & Control feature of Scalefusion. IT teams can mirror the device screen, connect to the end-user over a VoIP call to quickly resolve issues, or sync files. To support ITSM, IT teams can take screenshots or screen recordings and create context-aware support tickets. Scalefusion also offers Unattended Remote Cast and Control to manage your Windows devices without end user intervention. IT admins can initiate a remote control session even when the OS is down or the device is powered off with Scalefusion's integration with Intel vPro AMT Integration.

Inventory Overview, Reporting and Automated Alerts

When enterprise IT is in charge of a large device inventory that is spread across diverse geographical locations, it becomes strenuous to keep an individual track on all the devices. Scalefusion MDM offers a 360-degree overview of the entire device inventory which includes individual device details such as last connected time, Windows OS version, BIOS version, account & domain name, firewall & antivirus status etc.

IT admins can also generate contextual reports for various device parameters, including device availability, FileDock Analytics, and device vitals such as battery history and available and used storage.

Along with these reports, IT admins can automate recurring IT tasks- such as generating compliance reports, scheduling device reboots, and performing profile switches, using Scalefusion Workflows. The task automation capabilities can revolutionize the way IT teams manage a large device inventory- with minimum manual effort.

Summary

Windows devices are here to stay as they are the preferred choice for laptops and desktops across industries, from business to education. With more and more employees preferring to use their personal Windows devices to work, securing these devices and ensuring compliance is crucial than ever. Make the most of your Windows devices by bundling them with an appropriate, easy-to-use device management software. Choose Scalefusion Windows MDM for your work and school's Windows laptops and PCs.

Try it now for free

Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

Request a demonstration and see how Scalefusion can help you in managing your devices and securing your corporate data.

Book a Demo

About Scalefusion

Ambitious companies around the world trust Scalefusion to secure and manage endpoints including smartphones, tablets, laptops, rugged devices, POS and digital signages. Our mission is to make Device Management simple and effortless along with providing world class customer support.

Enterprise Sales & Partnerships

sales@scalefusion.com

partners@scalefusion.com

Call Us

US: +1-415-650-4500

UK: +44-7520-641664

NZ: +64-9-888-4315

India: +91-74200-76975