Scalefusion for Windows 10

Effectively Configure Windows 10 Devices for Business

Manage Windows 10-based computers, laptops and Point-of-sale systems with ease. Push necessary apps and content on Windows 10 devices and make them work for your business.

Overview

Manage Windows 10 devices in an enterprise environment. Push business-specific applications, security policies and configurations to heighten employee productivity on Windows 10 devices.

Benefits

- Drive faster device enrollment into corporate policies
- Run the device in single or multi-app kiosk mode
- Drive application management for public and enterprise apps
- Reduce employee distractions with browser configuration and application whitelisting
- Drive enhanced security for corporate data
- Push relevant business content with ease
- Quickly resolve device issues with Remote Troubleshooting

Introduction

Scalefusion MDM empowers enterprise IT teams to configure and manage Windows 10 laptops and computers for business. Through 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 Windows 10 devices is streamlined. IT admins can create a team-wide or enterprise-wide application usage policy, can control the browsing experience on browser kiosks as well as on devices used by employees. Scalefusion aids the IT teams in provisioning the Windows 10 devices with security settings, network configurations and business resources to ensure that employees can start working instantaneously.

Windows 10: The Chosen One

End-users- be it employees or customers, who deal with digital devices for business enjoy familiarity. Windows 10 holds more than 45% of the market share in desktop operating systems, which makes it evident that end-users still prefer Windows 10 over the rest. When Microsoft launched Windows 10, it took into consideration the ‘mobile-leaning’ user behavior and hence incorporated light-weight, clutter-free and seamless user experience specially designed to suit the Gen Z users. More and more cloud-centric features were introduced, making the Windows 10 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 10 devices in enterprises have become a key concern for enterprise IT admins.

While managing Windows 10 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 10 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 10 device management.

Scalefusion for Windows 10 Device Management

Windows device management has never been straightforward and IT teams often struggle in striking the right balance between management and excessive control hampering device usability. But thanks to the arrival of Windows 10, Windows device management has steadily transitioned from being super complex to fairly understandable, cost-effective and not network-restricted. Leveraging these capabilities, Scalefusion Windows 10 MDM offers an effective and easy way to manage the Windows 10 devices used in an enterprise environment.

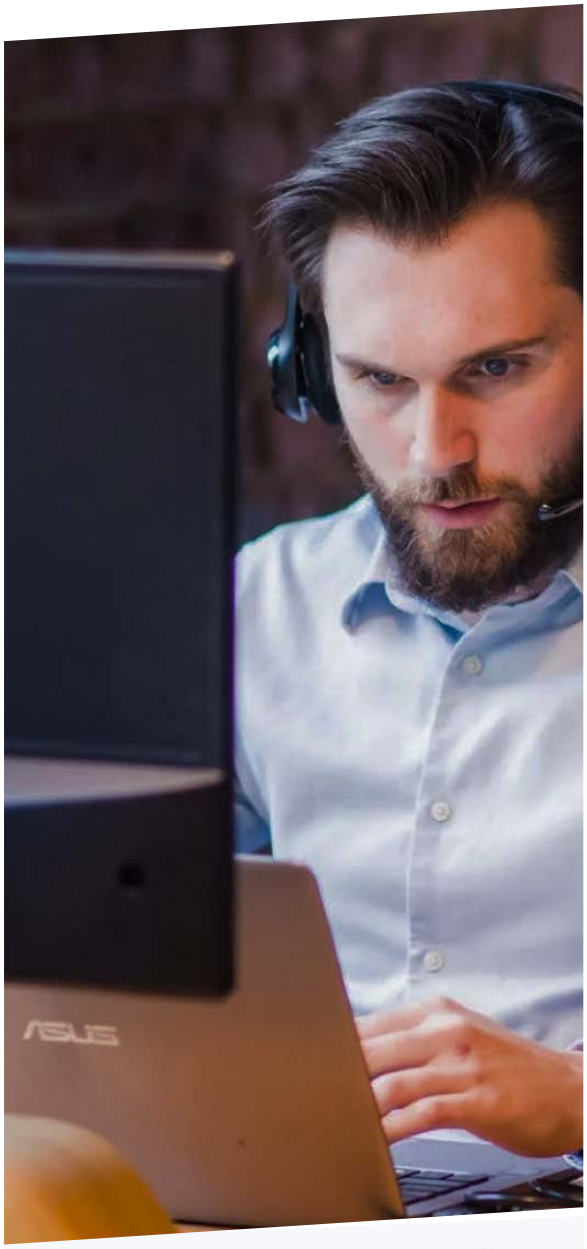
Primarily, the Windows 10 device management should focus on solving critical and most urgent IT needs- from easy enrollment to application delivery, security management to reporting. Scalefusion MDM for Windows 10 goes above and beyond the basic requirements from an MDM and presents a centralized management console to ease the task for enterprise IT admins.

1. Easy Enrollment

With Scalefusion, IT teams can choose to enroll and provision individual Windows 10 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 of managed devices into a faster and reliable security for its end users. With the configuration of SAML, Scalefusion allows its end users to access dashboard as well as the managed devices using SSO (single Sign on) using Okta, Office 365 AD, G Suite or PingOne IdP.

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



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

2. Policy Configuration, Utility Configuration and Updates

- **Utility Configuration**

Once the Windows 10 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 anytime. This configuration includes:

- Pushing of 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 and Powershell Scripts**

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 10 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 10 devices.

The MDM agent can be also 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 10 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. Scalefusion supports Add, Replace & Delete operations of CSP.

- **OS updates**

IT admins can control OS update rollouts and schedule the updates for particular time and day ensuring non-intrusive OS updates.

3. Single App Kiosk Mode

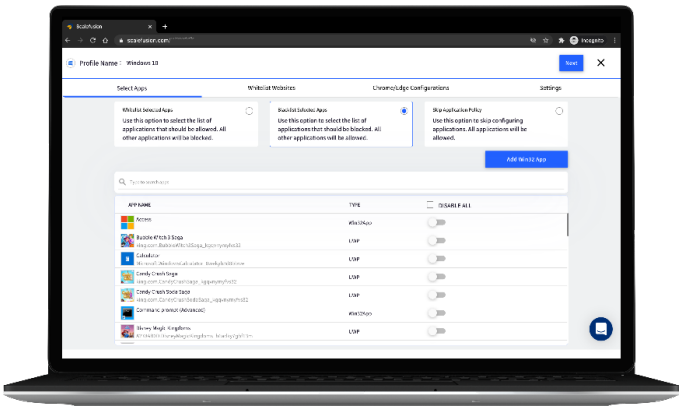
So far, we've discussed the settings available within Scalefusion MDM when Windows 10 devices are used by employees. But one of the other popular use-cases of Windows 10 devices is as kiosks. These kiosks can be deployed as wayfinders in public places, as a part of the POS system or as a public browser. To ensure the security and business usability of Windows 10 kiosks, Scalefusion MDM offers a single app kiosk mode.

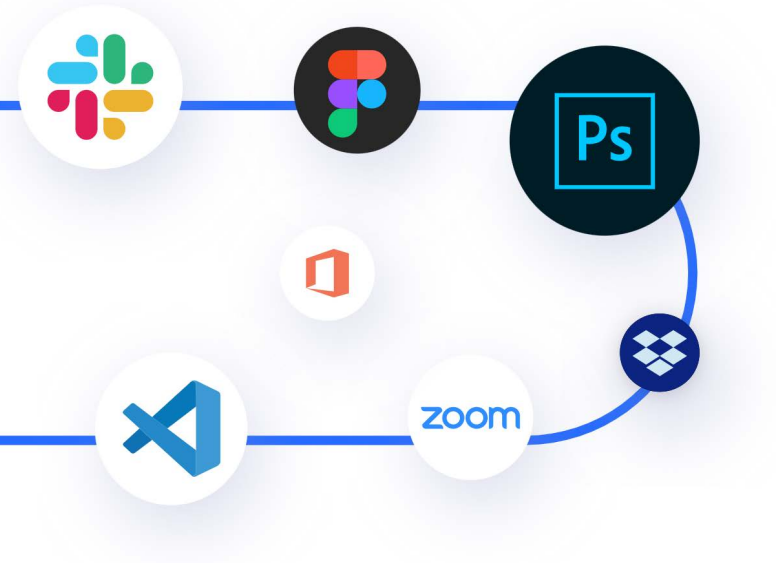
In the single app kiosk mode, the Windows 10 device is configured to run only one app at all times. This app can be a-

- Win32 app
- Pre-installed app
- Enterprise/ Third-party app
- Browser app- Google Chrome, Windows Kiosk Browser, Microsoft Edge Browser

4. Application Delivery

One of the prime reasons why IT teams want to manage Windows 10 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 Win 32 apps via the Windows Business Store on the managed devices at the time of enrollment, as well as later any time during the device lifecycle. IT admins can also install a private line of business apps on managed devices including UWP and MSI apps.





5. Website Whitelisting & Browser Configuration

With Scalefusion MDM for, IT teams can ensure secure browsing on the entire Windows 10 device inventory- be it deployed as a kiosk or as a device for employees. Within the Google Chrome Browser, IT teams can populate a list of allowed websites, blocking all the other websites. This not only helps in reducing distractions at work but also enables safe browsing, mitigating the threat from malware attacks from untrusted websites.

Scalefusion MDM offers configuration settings for Google Chrome and Microsoft Edge browser. IT admins can customize the startup settings, bookmarks, cookie policies and other privacy settings on both these browsers.

6. Application Whitelisting and Blacklisting

Downloading unidentified apps on devices can serve as an invitation for malware, possessing 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.

7. Content Management

For remotely working employees, streamlined access to business documents is critical. Similarly, Windows 10 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.

8. Extensive Security Configuration

After covering for security vulnerabilities that arise from accessing unknown websites and apps, IT teams can further secure the enterprise Windows 10 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 and a period after which it needs to be changed, and enforce it on the device inventory. Further, the IT can control search settings using Cortana, device peripherals like Camera, USB and Bluetooth.

Here's a list of security features available for Windows 10 devices managed with Scalefusion:

- **Windows Information Protection**

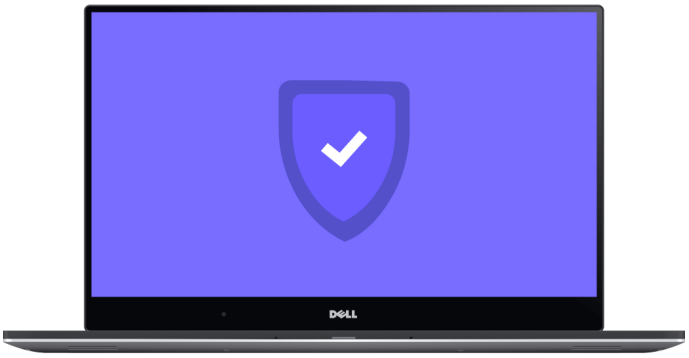
For securing corporate data, Scalefusion helps IT leverage the Windows Information Protection policy (WIP). While configuring WIP policies for Windows 10 profile, IT admins can define apps, domains, file types and enterprise cloud sources and the data from these will always be encrypted. The data can be read only via the predefined apps and copy/pasting of any data from these sources will be blocked.

- **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 the 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 is essential. With Scalefusion, IT admins can configure a VPN provider (native or third-party) for managed Windows 10 devices and route the traffic to the corporate apps and data via a secure network. IT administrators can also selectively enforce per-app VPN.



- **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 10 devices. End-users can use user gestures such as PIN, biometric authentication like a fingerprint or facial recognition to sign in to their managed Windows10 devices instead of a password.

- **Windows Defender Policies**

IT admins can add an extra layer of protection to the managed Windows 10 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.

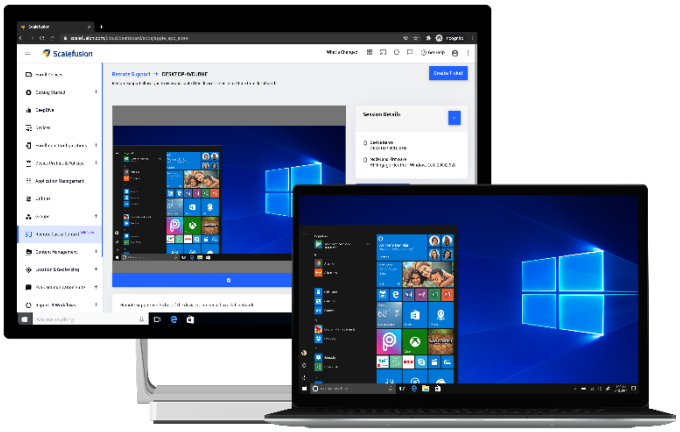
- **Certificate Management**

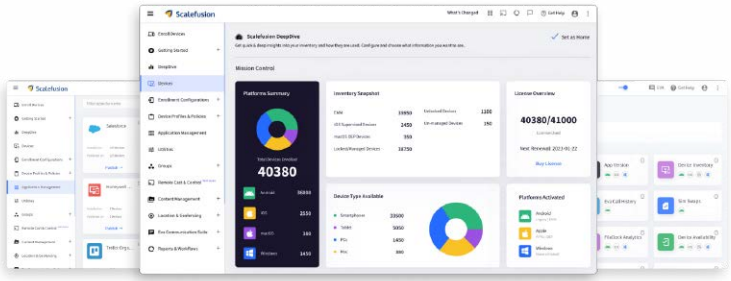
With Scalefusion MDM you can enhance the deployment experience of Digital Certificates on devices, as well as provide enterprises additional features and benefits of implementing security across devices. Using the Certificate Management feature helps, IT admins can streamline the process of deploying Digital Certificates to end-users' 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.

9. Remote Troubleshooting for Windows 10

Troubleshooting device issues is one of the regular IT activities. For large device inventory with remotely operating devices, the troubleshooting largely depends on the device issue described by the end-user. If the IT teams are unable to comprehend the device issue, it has to be fetched to the service center incurring higher device downtimes and added costs. Scalefusion streamlines Windows 10 troubleshooting over the air using the Remote Control feature. IT admins can mirror device screens on the dashboard to understand the device issue, take control of the device screens to perform actions, take screenshots and create context-aware support tickets on the integrated ITSM tool. With the Remote Control feature, IT teams can achieve significantly lower device downtimes.





10. 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.

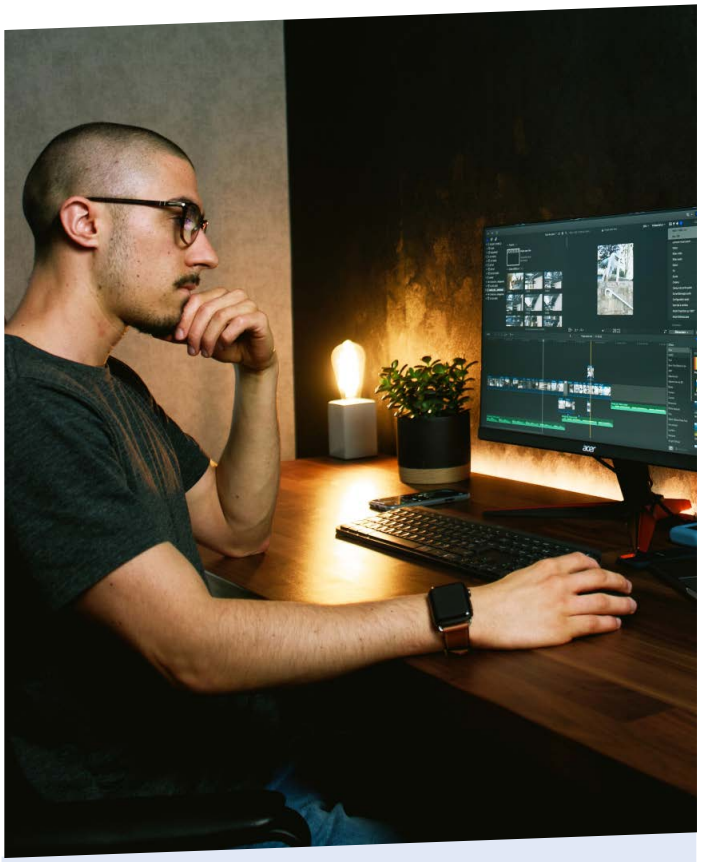
IT admins can also generate contextual reports for various device parameters including device availability, FileDock Analytics, device vitals such battery history, available and used storage.

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

Summary

Windows 10 devices are here to stay- being the preferred choice for laptops and desktops across industries, from business to education. With more and more employees preferring to use their personal Windows 10 devices to work, securing these devices and ensuring compliance is crucial than ever.

Make the most of your Windows 10 devices by bundling them with an appropriate, easy-to-use device management software. Choose Scalefusion Windows 10 MDM for your work and schools Windows 10 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) +1-650-273-5999

(INDIA) +91-8499-835020

Copyright© 2021 ProMobi Technologies. All rights reserved. Scalefusion, the Scalefusion logo mark appearing herein are property of ProMobi Technologies Pvt. Ltd. All other marks are the property of their respective owner/s.