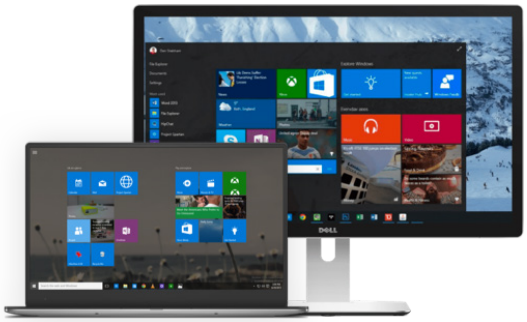
Scalefusion for Windows 10: Effectively Configure Windows 10 Devices for Business

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

- Enable employees to plug and work with pre-configured WiFi settings
- Allow or block UWP and Win 32 applications
- Run the device in single or multi-app kiosk mode
- Extensively configure Google Chrome to reduce employee distractions
- Control access to device peripherals and sharing
- Location tracking and geo-fences to avoid unauthorized access
- Push Email and Exchange settings to secure business mail

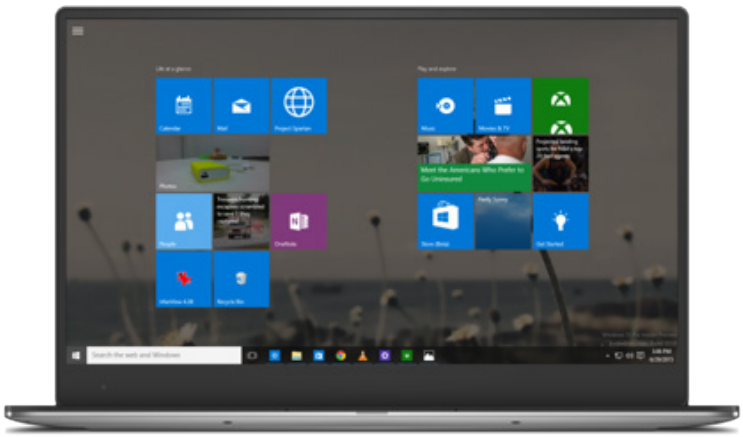
Introduction

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.



Try it now for free
Register for a free 14-day evaluation at 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

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.

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). IT admins can invite BYOD users from Azure AD for auto-enrollment.

This essentially saves 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.

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 WiFi 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.

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 apps and Win 32 apps 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.

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.

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 single app kiosk mode.

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

- Win32 app
- Pre-installed app
- Enterprise/ Third-party app
- Browser app- Google Chrome or Windows Kiosk Browser

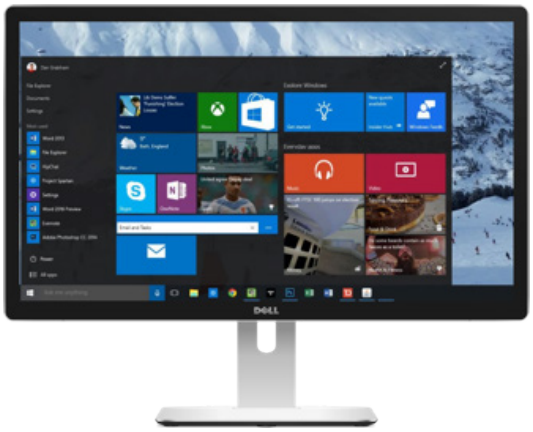
Website Whitelisting & Browser Configuration

With Scalefusion MDM, 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.

Extensive Security

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.



Try it now for free
Register for a free 14-day evaluation at 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

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. Along with these details, IT admins can automate recurring IT tasks- such as generating compliance reports, scheduling device reboot and profile switch. 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.

About Scalefusion

Scalefusion MDM allows organizations to secure & manage endpoints including smartphones, tablets, laptops, rugged devices, POS, and digital signages, along with apps and content. It supports the management of Android, iOS, macOS and Windows 10 devices and ensures streamlined device management operations with Remote Troubleshooting.

Scalefusion

Enterprise Sales & Partnerships
sales@scalefusion.com
partners@scalefusion.com

Call Us
(US) +1-650-273-5999
(INDIA) +91-8499-835020