ManageEngine
Browser Security Plus

WINDOWS 10 MIGRATION & COMBATING ITS IMPACT ON BROWSERS

ManageEngine
Browser Security Plus

Executive summary

With Microsoft's announcement to end Windows 7 support effective January 2020, there's only a handful of months left to get Windows machines up-to-date. As the deadline draws closer, IT admins have probably either completed the transition or devised a solid plan of action by now. But does the plan include a strategy to handle the change in default browsers? Starting with Windows 10, Microsoft Edge replaced Microsoft Internet Explorer (IE) as the default browser, bringing more compatibility problems with each legacy web application. This introduces a whole new problem for the IT admins to address, just after getting their fleet of Windows machines up-to-date. Since rendering legacy web applications relies on plug-in dependencies native to only legacy browsers, IT admins need a way to both render these legacy applications without breaks, while other web apps and websites can be opened with the safety that comes with modern browsers. This white paper will discuss how IT admins can achieve this without depending on end users to make the right choice of browsers.

Rise in browser-website compatibility issues

Windows 10 uses Edge as the default browser instead of IE. The change can't come soon enough, since IE is slow and filled with vulnerabilities waiting to be exploited. Knowing about the shortcomings of IE, it seems natural that IT admins would stay as far away from it as possible. However, this isn't the case. Most intranet web applications and websites were developed with plug-in dependency, and require a browser that still supports plug-ins; since IE fits the bill, IT admins need employees to use IE to render legacy web applications without experiencing breaks.

Because Microsoft installed IE as the default browser, IT admins only had to worry about the threats associated with it up to this point. With Windows 10, Edge replaced IE as the default browser, bringing more compatibility problems with each legacy web application. IT admins have two options to overcome compatibility issues:

- Educate users to open specific web applications with IE.
- Use Group Policy Objects (GPOs) to configure Enterprise Mode so legacy web applications get redirected to IE.

What is Enterprise Mode?

Enterprise Mode is a feature provided by Microsoft that allows IT admins to redirect certain websites from an Edge browser to IE, and vice versa. To do this, IT admins need to configure an XML file with a site list, a list of websites that will be forced to open in IE. This feature is aimed at avoiding compatibility issues for end users.

Achieving browser-website compatibility

As a simple solution, IT admins can direct users to open specific websites in IE and other websites in different modern browsers. Alternatively, they can configure Enterprise Mode to redirect certain websites to IE, while the remaining websites open in the default browser. The latter is more effective since it reduces slip-ups from end users and, ultimately, reduces help desk calls. However, for an IT admin, configuring the GPO is an arduous task.

Disadvantages of GPOs

1) Configuring and deploying Enterprise Mode is a tedious process.

IT admins first have to create a GPO and configure it using Enterprise Mode. Then, they have to create an organizational unit (OU), a container with computers or users, to which the configured GPO is to be deployed. Finally, they have to deploy the configured GPO to the OU. But the problem here is that Enterprise Mode requires IT admins to enter the websites that they want to redirect to IE. Adding these websites manually is a tiresome process. If an IT admin wants to apply different sets of websites for each department in their organization, it can take a long time and requires a lot of patience.

2) There isn't enough visibility into GPO deployment.

When the GPO is applied to an OU, IT admins have no way to find out if it was successfully applied. The current GPO layout is old and has an archaic interface, which does not provide proper visibility on the deployment status.

Using Browser Router in Browser Security Plus

Browser Security Plus, ManageEngine's comprehensive browser security software, is the ideal tool to maintain compatibility while ensuring security.

The Browser Router feature in Browser Security Plus helps redirect websites to specific browsers without the hassle of depending on GPOs. With Browser Router, IT admins can configure a policy defining the websites that need to be opened with IE, or just select the option to redirect all the intranet traffic to IE.

If they want to redirect different sets of websites for different departments in their organization, they can use website groups. Once configured, these website groups can be used across multiple instances within Browser Security Plus.

Although IE cannot be avoided, IT admins can make sure that it's used only when absolutely necessary with the Browser Lockdown feature, which enables admins to render websites in kiosk mode, and ensures that no other websites can be accessed during the session. If the IT admin creates website groups for different departments, the same groups can be rendered as kiosk browsers for each department. This way, IT admins can secure their network from vulnerabilities in IE and simultaneously maintain compatibility.

With browsers increasingly used on a daily basis, IT admins need to be completely sure that migrating to Windows 10 doesn't leave users with compatibility issues. Browser Security Plus can help ensure that users don't experience issues after the imminent migration.

Download a free, 30-day trial of Browser Security Plus to see how it fits in your organization, or request a free, personalized demo to understand its full capabilities.

Download **Schedule a demo**