Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications

4 out of 9 rated this helpful - Rate this topic

Published: June 24, 2013

Updated: August 28, 2013

Applies To: Windows Server 2012 R2

The explosion in use, number of consumer devices, and ubiquitous information access is changing the way that people perceive their technology. The constant use of information technology throughout the day, along with easy access of information, is blurring traditional boundaries between work and home life. These shifting boundaries are accompanied by a belief that personal technology—selected and customized to fit users' personalities, activities, and schedules—should extend into the workplace. To accommodate this growing need of personal consumer devices being connected to enterprise networks, Windows Server® 2012 R2 introduces the following value propositions:

- Administrators can control who has access to company resources based on application, user, device, and location.
- Employees can access applications and data everywhere, on any device. Employees will get single sign-on when using browser applications or enterprise applications.

Key concepts introduced the solution

Workplace Join

With Workplace Join, information workers can join their personal devices with their company to access company resources and services. When you join your personal device to your workplace, it becomes a known device and provides seamless second factor authentication and single-sign-on to workplace resources and applications. When a device is Workplace-Joined, attributes of the device can be retrieved from the directory to drive conditional access for the purposes of authorizing issuance of security tokens for applications. With Windows Server 2012 R2, Windows 8.1 and iOS devices can be Workplace Joined.

Device Registration Service

Workplace Join is made possible by the Device Registration Service (DRS) that is included with the Active Directory Federation Role in Windows Server 2012 R2. When a device is Workplace Joined, the DRS provisions a device object in Active Directory and sets a certificate on the consumer device that is used to represent the device identity. The DRS is meant to be both internal and external facing. Companies that deploy both DRS and the Web Application Proxy will be able to Workplace Join devices from any internet connected location.

For more information about deploying Device Registration Service, see Configure a federation server with Device Registration Service

Workplace Join as a seamless second factor authentication

Companies can manage the risk related to information access and drive governance and compliance while allowing consumer devices to access corporate resources. Workplace Joined devices provide the following capabilities to administrators:

- Administrators can identify known devices with device authentication which in turn can be used to drive conditional access and gate access to resources based on this information.
- Provides a more seamless sign-in experience to company resources from trusted devices.

Single Sign On

Single Sign on in the context of this scenario is the functionality that reduces the number of password prompts the end user has to enter when accessing company resources from known devices. This implies that users will be prompted only once during the lifetime of SSO when accessing company applications and resource. If a device is Workplace Joined, the user who is registered to use this device will get persistent SSO (for 7 days by default) when accessing company applications and resources from this device. This means user will have seamless sign-in experience within the same session or for the new sessions.