Microsoft BYO's Offering

Contributed by David Noel-Davies

One of the biggest trends in IT today is that Bring Your Phone Device trend. Unless you have been living under a rock, you know that users are demanding to be able to access corporate resources from personal consumer electronics devices. Furthermore, they expect access whether they are working on premise in the office, or remotely.

Obviously this trend presents some significant challenges for IT staff who have long had a monopoly on device provisioning. IT pros must deal with everything from Wi-Fi saturation (related to an ever increasing number of devices), IP address depletion, and a whole slew of authentication and access control issues.

One of Microsoft's goals in creating Windows Server 2012 R2 was to give administrators some tools that they could use to cope with the Bring Your Own Device trend. One of the most helpful of these tools is something called workplace join. In this article series, I will explain what the workplace join feature is, why it is helpful, and how you can implemented in your own organization.

The key to understanding the workplace join features usefulness is to understand a little bit about the history of Active Directory. Active Directory was actually designed back in the 1990s, and it made its debut with Windows 2000. As such, the Active Directory was born at a time when PCs were basically the only game in town. At that time, there weren't any tablets or smart phones (at least not as they exist today) so the thought of allowing devices other than PCs to join an Active Directory domain probably never even crossed the design team's minds.

Of course this raises the question of why domain membership even matters. When a PC is joined to an Active Directory domain, a computer account is created within the Active Directory database. This computer account functions very similarly to a user account. It uniquely identifies and authenticates the corresponding computer.

When a user logs into the Active Directory, Windows looks at both the username and the computer name. Assuming that the user is authenticated successfully, Windows retrieves the user specific and computer specific group policy settings and combines them into the effective policy for the user session. In other words, group policy based security is tied both to the user and to the device that they are using.

Group policy usage is far from being the only justification for joining a computer to the Active Directory. There are a number of different management tools that require domain membership in order to work. Even so, let's talk about group policy based security a little bit more.

The problem with allowing a user to login from a non-domain joined device is that device level security policies are not applied. Several years ago, Microsoft began to realize that this was a problem and actually designed a version of Windows Mobile to support domain enrolment.

Domain enrolment was a little bit different than a true domain joined. Without getting into all of the nitty-gritty details, the biggest difference was that domain enrolment was geared toward smart phones. Because smart phones were not running true desktop operating systems, the vast majority of the group policy settings that are normally applied to devices were irrelevant. At the same time however, there are certain security settings that are specific to mobile devices that don't appear in a standard group policy. That being the case, enrolling a Windows Mobile device into the Active Directory allowed the device to participate in the Active Directory domain, and allowed it to receive a set of Windows Mobile

specific security policies.

Ultimately the concept of domain enrolling a smart phone went away. The concept was only applicable to Windows Mobile devices, which made it unsuitable for global mobile device management. Eventually however, Microsoft rolled the technology that was initially used for domain enrollment into other technologies such as Windows ActiveSync and Windows InTune.

Today, Windows ActiveSync and similar technologies make it possible to apply security policies to a variety of mobile devices. Just about every smart phone supports ActiveSync policies regardless of the manufacturer. There are differences in the degree of support because not every model of smart phone supports every available ActiveSync policy, but ActiveSync has provided a somewhat consistent way for administrators to secure consumer devices.

In spite of these capabilities, consumer devices that are secured with ActiveSync do not truly participate in the Active Directory. Devices are not domain joined, nor are they Active Directory enrolled.

This is all about to change in Windows Server 2012 R2. Microsoft is introducing a new feature called workplace join. Workplace join can be thought of as a next generation alternative to joining a PC to the Active Directory. Rather than an administrator having to provision a PC for domain membership, the workplace join feature allows end-users to self-provisioned mobile devices in a secure manner.

The workplace join feature is based on the Active Directory Federation Service, which essentially acts as an authentication and access control mechanism for end-user devices.

Even though a workplace join works differently than a legacy domain joined, end user devices become true Active Directory members. When an end user joins a device to a domain, Windows Server creates an Active Directory object for the device. This object is associated with the user account for the user who owns the device. Furthermore, a special certificate is installed on the mobile device, and the certificate is associated with the devices object within the Active Directory. This allows the device to be positively identified.

So with this in mind, you might be wondering about the benefits of allowing end-users to join devices to the Active Directory using a workplace join. After all, basic security can be implemented through ActiveSync policies, so what does the workplace join feature bring to the table that ActiveSync policies do not?

There are a number of different benefits to using workplace join. I’m going to wait to cover some of these benefits until a little bit later on in the series when I have shown you how to deploy the required infrastructure. For right now though,

there are three primary benefits that I want to share with you.

The first benefit is single sign-on. Users are able to access various corporate resources without having to authenticate separately for each resource.

The second benefit is that it gives the end users the flexibility to use whatever device they want, but it still allows the IT department to adhere to its established security policies. I'll talk a lot more about this one as the series progresses.

The third benefit, and this is a biggie, is that an administrator can conditionally grant users access to resources. To give you a quick example of how this might work, let's imagine that because I am a Microsoft MVP I had some serious bias toward the iPad and did not want to let anyone access network resources from an iPad. It would actually be possible to put a policy into place that would allow a user to access certain resources from a PC, a Surface Tablet, or maybe even a Windows Phone, but not from an iPad.

Obviously this is a ridiculous situation that could probably never be justified in real life, but I threw it out there to underscore the point that the administrator ultimately has control over device usage. If as an administrator there are certain types of devices that you consider to be insecure (or that you do not want to support) you can limit access for those device types. You can block access completely, or you can limit access to certain resources.