CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

Centrify®

DELL Software

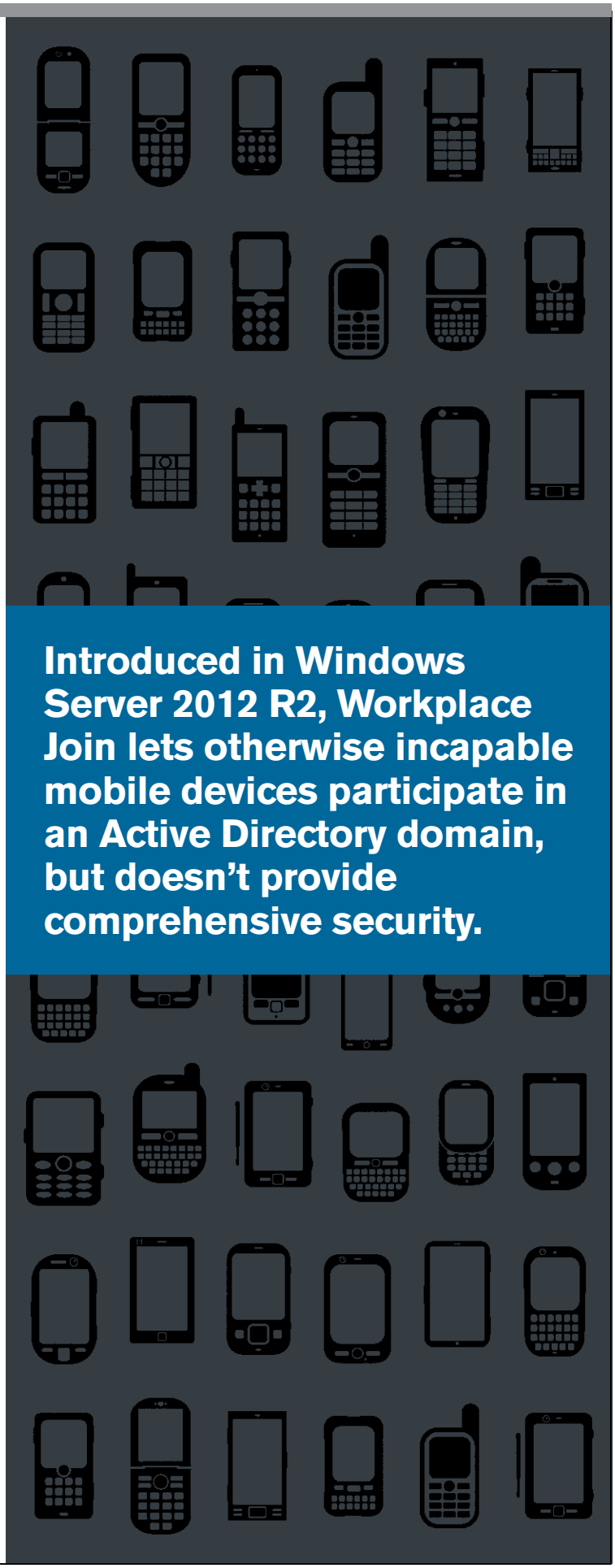
Mobile Management with Active Directory

A useful feature in Windows Server 2012 R2 joins AD and mobile devices, but management can be a bit tricky.

1105 MEDIA

Manage Mobile Devices and Policies in Active Directory

BY BRIEN M. POSEY



Introduced in Windows Server 2012 R2, Workplace Join lets otherwise incapable mobile devices participate in an Active Directory domain, but doesn't provide comprehensive security.

One of the major challenges facing organizations today is the proliferation of mobile devices. Mobile device use raises a number of concerns around issues such as security and privacy. Although there are a number of different solutions available from Microsoft and from third-party vendors for mobile device management, IT shops are increasingly finding that achieving the desired level of security requires them to adopt multiple solutions.

In order to understand the advantages and disadvantages of the available solutions, it's important to understand why mobile devices pose such a challenge in the first place. Mobile devices are different from

desktop PCs in that they typically cannot be joined to an Active Directory domain. When a PC is joined to the Active Directory domain, a computer account is created as a means of authenticating and positively identifying that computer as it participates on the network. Furthermore, applying Group Policy settings can secure the computer's OS, and access control lists provide a mechanism for controlling access to network resources at the computer level.

Mobile devices are the complete opposite. They can't be joined to the Active Directory domain (at least not in the traditional sense) and, therefore, you can't apply Group Policy settings to a mobile device.

ActiveSync has become an industry standard for providing synchronization between Exchange and mobile devices.

Previously, one of the best options for securing mobile devices that participate on a corporate network was the use of ActiveSync policies. For those who might not be familiar with ActiveSync policies, they were first introduced in Exchange Server as a mechanism for pushing mail to mobile devices. Eventually, Microsoft extended the ActiveSync protocol in an effort to allow security settings to be applied to mobile devices.

The Trouble with ActiveSync

ActiveSync has become an industry standard for providing synchronization between Exchange and mobile devices. Every major device manufacturer supports the use of ActiveSync policies as a way of locking down their devices. However, there are a couple of issues that limit ActiveSync as a comprehensive mobile device security solution.

The first issue is that mobile devices support ActiveSync in varying degrees. ActiveSync policies are made up of a collection of individual policy settings. Most of the mobile devices available today do not support every available policy setting. As such, administrators aren't assured that a policy setting will apply to every device that's in use on their network unless they restrict access to devices that do not fully support all policy settings (which includes most device types). The various ActiveSync policy settings and the devices that support them are published in a Wikipedia post at **bit.ly/1rHOUk3**.

Another issue with using ActiveSync for mobile device security is that it has become increasingly difficult to fully implement. Exchange

Server 2013 and Microsoft Office 365 expose ActiveSync policy settings through mobile device mailbox policies. Microsoft makes it relatively easy to create mobile device mailbox policies, but the Exchange Server 2013 Administrative Center and the Office 365 Exchange Admin Center only expose the most basic policy settings (see **Figure 1**). These are the policy settings that are used to require a password and to set password-related attributes, such as the minimum password length. There are dozens of other ActiveSync settings available, but using them means delving into Windows PowerShell (or reverting to Exchange Server 2010).

The Workplace Join feature enables device-level access control.

Organizations that create comprehensive mobile device mailboxes usually find that those policies work really well for securing mobile devices. Even so, ActiveSync has its limits. For instance, ActiveSync doesn't allow for device-level access control for resources that exist outside of Exchange Server.

Pluses and Minuses for Workplace Join

One of the new features in Windows Server 2012 R2, called Workplace Join, is a way for allowing otherwise incapable mobile devices to participate in the Active Directory domain. Even though a device such as an iPad or a Windows RT tablet can't join to an Active Directory domain in the same way a Windows desktop PC can, the Workplace Join feature lets these types of devices participate in Active Directory in other ways.

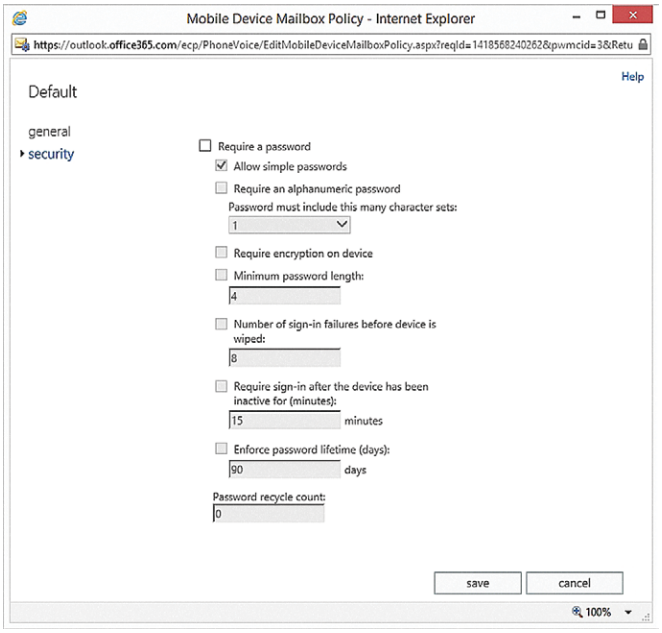


Figure 1. *Office 365 exposes only the most basic ActiveSync policy settings.*

The Workplace Join feature accomplishes three main things. First, it allows a device to be positively identified on the network. When a user enrolls a mobile device, a certificate is assigned to that device. This certificate is used as an identification mechanism. The device is also added to Active Directory and is listed in the Enrolled Devices container.

Second, the Workplace Join feature enables device-level access control. It's possible to base access to Web applications on whether the device has been enrolled in Active

Directory. This isn't done through standard access control lists, but rather as a function of Active Directory Federation Services and a relaying-party trust. Third, Workplace Join provides single sign-on capabilities for certain network resources.

Unfortunately, Workplace Join is inadequate by itself. Although it does provide some interesting capabilities, it also lacks some key features that are required for organizations to effectively manage mobile devices. Keep in mind Workplace Join is designed to simplify resource access. As such, it's not a true mobile device security feature. For instance, Workplace Join doesn't provide a collection of Group Policy settings that can be applied to mobile devices. Similarly, it doesn't provide the types of device security controls that are available through ActiveSync policies.

Workplace Join is designed to simplify resource access. As such, it's not a true mobile device security feature.

Workplace Join is also inadequate as an access control mechanism. While it's true Workplace Join can be used to grant or deny access to network resources based on device enrollment, there are significant limitations. You cannot, for instance, use an access control list to block devices that aren't enrolled. Most often Workplace Join is used to control access to browser-based apps.

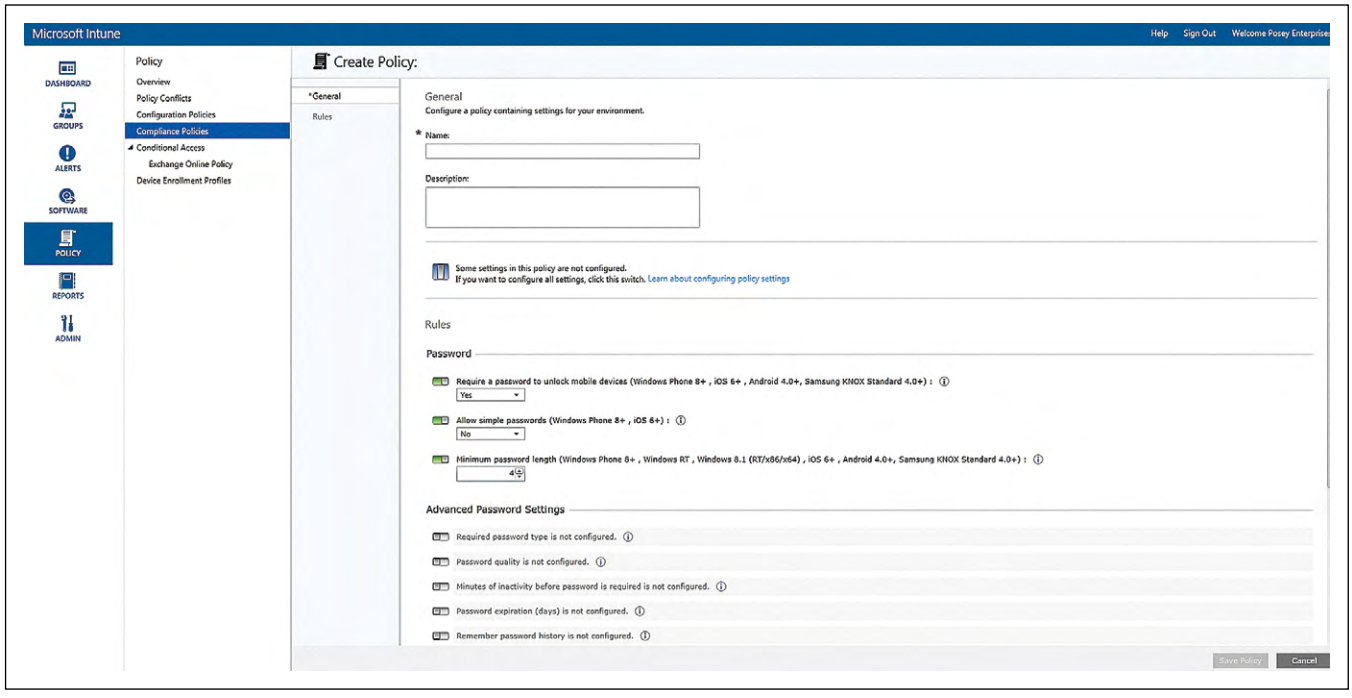


Figure 2. *Microsoft Intune policies are similar to ActiveSync policies.*

Moving to a Primary Solution

Workplace Join and ActiveSync policies both have their place, but the primary Microsoft solution for securing and managing mobile devices is Microsoft Intune (formerly known as Windows Intune). Microsoft Intune is a cloud-based service that can apply security controls to user devices. These controls are very similar to those that are available through ActiveSync (see **Figure 2**). Unlike raw ActiveSync, however, Intune is also able to create template-based policies that can be applied to various types of mobile devices (see **Figure 3**).

Workplace Join and ActiveSync policies both have their place, but the primary Microsoft solution for securing and managing mobile devices is Microsoft Intune.

Microsoft Intune is also able to manage applications on mobile devices. For example, the organization's approved applications can be made available to mobile devices. Administrators also have the ability to blacklist undesirable applications.

So what should you be using to manage your network–Microsoft Intune, Exchange Server, Workplace Join or perhaps something else? For the best overall management experience, you might want to use a combination of all three. All three technologies have both abilities and limitations. However, the three technologies complement one another rather nicely.

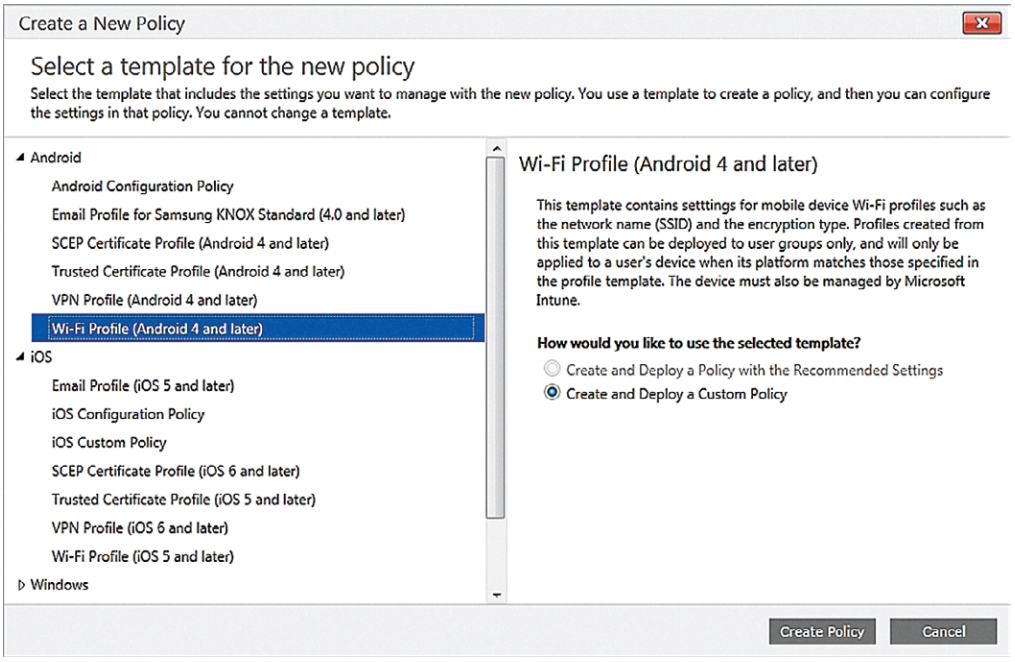


Figure 3. *Microsoft Intune can create template-based policies for mobile devices.*

On the surface, there seems to be a high degree of overlap between the three solutions. Microsoft Intune, for example, provides the ability to enforce password policy settings on mobile devices, but so does ActiveSync. Similarly, the Workplace Join feature provides access control to Web-based applications, but Microsoft Intune also provides application access control capabilities.

Although there are some similar capabilities exposed through the various management platforms, the overlap helps to provide good, comprehensive security for mobile devices. The reason why overlapping features may be necessary is because mobile devices can exist in different states.

A user could easily synchronize the device to Exchange Server without ever enrolling the device in Active Directory.

Imagine for a moment that a user wants to access e-mail and the calendar running on a mobile device. Because ActiveSync is an Exchange Server feature, a user could easily synchronize the device to Exchange Server without ever enrolling the device in Active Directory. Doing so would provide the user with access to his mail, calendar, contacts and even his task list.

In this type of situation, the ActiveSync policy settings are the only security mechanisms readily available to prevent sensitive information from the user's mailbox from being exposed should the user's device be lost or stolen. Remember, the user is able to access the full contents of his mailbox without ever performing a Workplace Join.

Although the user can access quite a bit of data without ever performing a Workplace Join, the user's abilities are also somewhat limited. Sure, the user can access the contents of his mailbox (including the calendar, contacts and task lists), but can't access any other network resources. This is where the Workplace Join feature comes into play.

Oftentimes administrators use the Workplace Join feature as an access control mechanism for users who are accessing Web applications from outside the organization. Organizations with large SharePoint deployments in place are probably the best example of this. If a user attempts to log into SharePoint from a desktop computer that exists inside the organization's firewall, the user's Active Directory credentials are normally used to authenticate the user directly into SharePoint.

In the past, connectivity to SharePoint Sites has worked similarly for a user connecting from outside the organization. The user would enter a URL for the SharePoint Site, and then be asked to enter her Active Directory credentials to gain access to the site.

The Workplace Join feature provides an extra layer of security. The network can be configured to deny access to SharePoint content for devices that aren't enrolled in Active Directory. This is a great way of preventing users who are working on unauthorized devices from accessing SharePoint resources or other Web-based resources.

Microsoft Intune is a management tool that provides a single pane of glass for managing a variety of mobile devices.

So what about Microsoft Intune? Microsoft Intune is a management tool that provides a single pane of glass for managing a variety of mobile devices. Microsoft Intune offers a self-service portal where a user can access applications or perform functions such as a device wipe or the deployment of an application to his mobile device.

Redmond's recommendations for Microsoft Intune have changed considerably over the years. The company's current recommendation is that you use ActiveSync to secure any device that isn't enrolled in Active Directory via Workplace Join. Microsoft Intune is primarily designed to manage devices that have been enrolled in the Active Directory.

Remember, though, Microsoft Intune is designed to act as an organization-level management solution for mobile devices, and it would be counterproductive to use two separate solutions for mobile

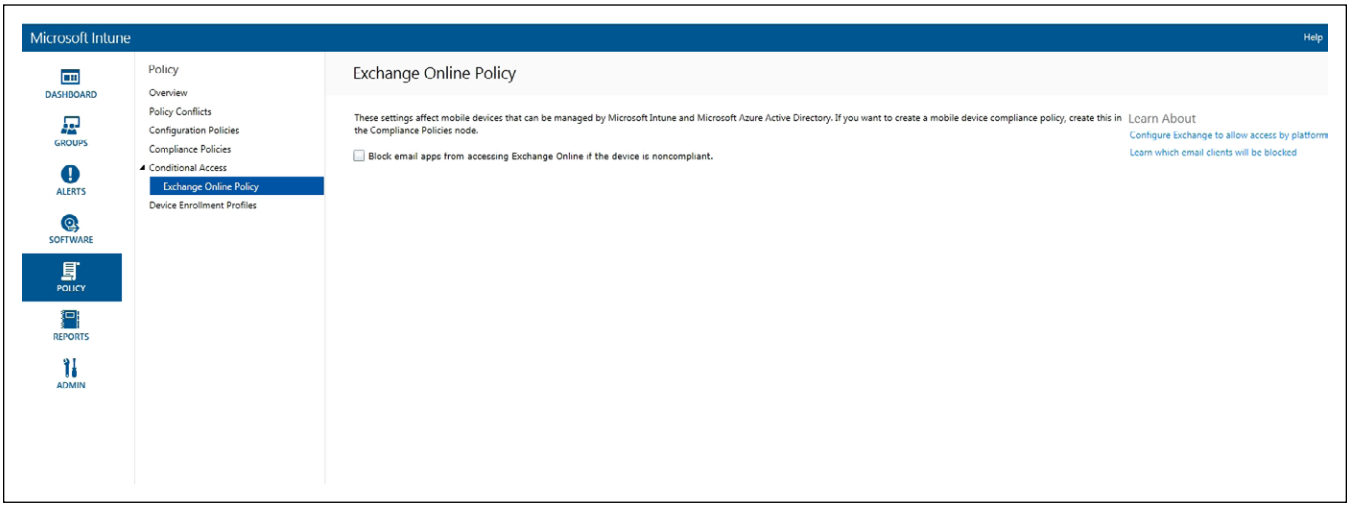
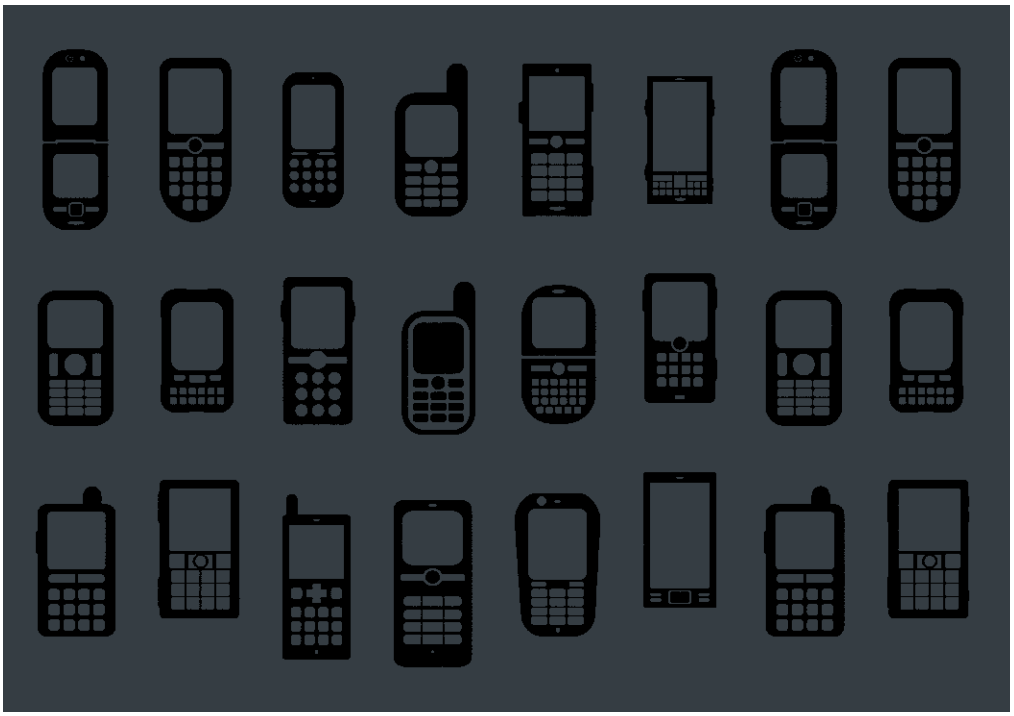


Figure 4. *You can block non-compliant devices from accessing Exchange online.*



It's possible to manage non-enrolled devices using Microsoft Intune.

device management (ActiveSync for devices not enrolled and Microsoft Intune for devices that have been enrolled).

Fortunately, it's possible to manage non-enrolled devices using Microsoft Intune. The trick to doing so is to use the Microsoft Exchange Connector. This connector ties Microsoft Intune to Exchange Server so that Intune can be made aware of devices that are being used to access Exchange Server resources, but aren't enrolled in Active Directory. That way, non-enrolled devices can be managed alongside devices that have been enrolled. In case you're wondering, it is possible to block e-mail apps on non-compliant devices from accessing Exchange.

Benefits and Limitations

The fact that mobile devices aren't domain-joined in the traditional sense makes mobile device management tricky. The tools and techniques used for mobile device management will likely change as time goes on, but for the time being, Microsoft has given us several good tools for managing device security and access control to network resources. R

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.

To Join or Not to Join?

Suppliers of mobile device management and Active Directory management tools have various levels of support for the new Microsoft Workplace Join feature.

BY JEFFREY SCHWARTZ

Various suppliers of mobile device management software and Active Directory administration tools say their offerings provide more comprehensive methods of authenticating mobile and user-owned devices.

Microsoft introduced Workplace Join in Windows Server 2012 R2 to make it easier to connect employee-owned tablets and smartphones and other device types not designed to join an Active Directory domain—notably iPads and Android-based tablets and phones. Of course, that also includes Windows RT tablets and phones based on the Microsoft Windows Phone OS.

Workplace Join allows administrators to join personal devices providing two-factor authentication and single sign-on to enterprise network resources and applications. When enrolling a device using Workplace Join, Active Directory can retrieve the attributes of that device providing "conditional access for the purpose off authorizing issuance of security tokens for applications," according to Microsoft.

But as the article, "Manage Mobile Devices and Policies in Active Directory" (p. 1), on how to implement Workplace Join warns, it has limitations. Workplace Join is only designed to simplify resource access and is not intended as a complete mobile device security feature. It also doesn't provide Group Policy settings that can be applied to mobile devices, has limited access control mechanisms and doesn't provide the types of device security controls available with ActiveSync polices.

For its part, Microsoft doesn't market Workplace Join as a mobile device management solution, though it's enabled in the company's own new Enterprise Mobility Suite, and specifically the Intune management service, so perhaps it might become a requirement in the future.

"Right now I don't see many customers adopting it."

Tomas Vetrovsky, Director of Product Management, Mobile Iron

Third-Party Options

Various suppliers of mobile device management software and Active Directory administration tools say their offerings provide more comprehensive methods of authenticating mobile and user-owned devices. Those tools typically use various means of connectivity including Microsoft Exchange ActiveSync, Apple Push Notification Service (APNS) and Google Cloud Messaging (GCM). Whether Workplace Join becomes a preferred means of enrolling mobile devices in Active Directory domains remains to be seen.

So far, integration between Workplace Join and third-party tools is at a formative stage. A few offer it in some form, while others don't see a need for it at this point. Chris Ashley, a product manager at Dell Software, says customers have inquired about Workplace Join support. "Among customers I have actually talked to, they're actually excited about this feature, they're just holding off mostly because of the fact they're still running a lot Windows 7 desktops," Ashley says. "But it's something they want to introduce. A feature like this is really cool, but sometimes you do find those little shortcomings that make it a procedure."

Dell last month released a new module for its Active Administrator tool for Active Directory management. The new module aids in the management of a certificate, which is a key part of setting up Workplace Join, according to Ashley. It will install the certificate on the server so when it expires, an administrator can update it. The new module also makes it possible to assign access to resources via IP

addresses. The benefit of using Active Administrator, Ashley notes, is that it supports management of Group Policy Objects.

"Certainly any policies that you use to provide access to the servers internally, we can cover," he says. "We're able to manage those policies, to recover them if they're messed up and give it confidence to change those policies because we can roll those polices back, if the change has a detrimental effect."

The new module, called Active Administrator for Certificate Management, provides DNS management capability in addition to certificate management. "The DNS management capability is important because there are two records that you have to create to make sure devices that are trying to register with Workplace Join can actually locate the machines that are required," Ashley says. "So being able to manage those records, and monitor that those records exist and that they can be reached will also be important to folks who are trying to leverage Workplace Join."

"Our customers would like to use Workplace Join, mainly for single sign-on, but right now I don't see many customers adopting it."

—Tomas Vetrovsky, director of product management at MobileIron

Down the road, Ashley says Dell is evaluating how its tools, which in addition to Active Administrator include GPO Manager, might add more security to devices registered using Workplace Join. An example would be more refined policy management, but factoring into that will be new capabilities delivered by Microsoft in the next release of Windows Server and Windows 10, as well as customer demand.

Mobile Device Management

Tomas Vetrovsky, director of product management at Mountain View, Calif.-based MobileIron, a supplier of mobile device management software, says customers have inquired about integrating its namesake software with Workplace Join. "Our customers would like to use Workplace Join, mainly for single sign-on," Vetrrovsky says. "But right now I don't see many customers adopting it."

With MobileIron software, while it connects to Active Directory, once the authentication is established, it handles management and policies, he says. In and of itself, Workplace Join wasn't designed to work with GPOs, Vetrovsky adding it doesn't need to when using mobile device management (MDM). "The GPO-based approach was designed for devices that are connected on the local area network," he says. "As soon as you start talking about tablets or laptops that are spending most of the time somewhere on the Internet, just connecting from the

outside, MDM provides real-time management that's better than the GPO approach."

Another major MDM supplier that will integrate with Workplace Join is Good Technology, but Eugene Liderman, the company's director, public sector technology, says users of the Good Dynamics Secure Mobility Platform don't need it.

"Good can be complementary to Workplace Join or operate completely independent of it," Liderman says. "If you look at the majority of what Workplace Join provides, which is visibility to enrolled devices, some basic device-level control and single sign-on to certain back-end resources, all of this can be provided by the Good Dynamics Secure Mobility Platform. The major difference is that Good provides this without having to upgrade the Active Directory schema like Workplace Join requires."

Good Dynamics respects the user-state in Active Directory when a user requests network access.

Liderman adds that Good Dynamics respects the user-state in Active Directory when a user requests network access. For example, if a user is removed/suspended/deactivated in Active Directory, its tools will prevent that user from gaining access to network resources/data/messages. In addition, he says while Workplace Join focuses on device-level control, Good Dynamics can support device-level control via MDM. "More important, it can also enable application-level controls and policy management, as well as single sign-on access to various back-end resources whether through Good's secure browser or through a native iOS or Android application secured with the Good SDK," he says.

Customizable Policy Management

Paul Moore, co-founder and chief technology officer at Centrify Corp., says Workplace Join is very similar to the mobile device enrollment in the Centrify Suite, but the latter offers more customizable policy management. "An admin can set up devices so that they have zero sign-on to corporate resources, but still have precise control over what users can do," Moore says. "For example, an admin can indicate that an app is only accessible from enrolled devices, at certain times of the day, from particular device types, from specified countries, etc."

Centrify also offers full device management capabilities, with features including remote wipe, lock and find for end users, and centralized policy management for administrators, he says. The centralize policy

management permits the configuration of e-mail settings, the installation of applications, VPN setup, device restrictions and so on.

No Workplace Join Integration

Blake Branon, lead solutions engineer at AirWatch, acquired by VMware Inc. last year, says AirWatch provides more advanced security controls via the AirWatch Secure Email Gateway (SEG). The gateway enforces granular policies to allow or disallow access to corporate content, as well as such variables as device type, OS, encryption and whether a device is jail broken. It does make use of access control lists (ACLs), as well as Windows PowerShell support. "AirWatch and Workplace Join are mutually exclusive so a customer would either use Workplace Join and manage it with Active Directory or use AirWatch," Branon says.

"AirWatch and Workplace Join are mutually exclusive so a customer would either use Workplace Join and manage it with Active Directory or use AirWatch."

–Blake Branon, lead solutions engineer at AirWatch

Others who question the need to use or integrate with Workplace Join are Renee Bradshaw, senior solutions marketing manager at NetIQ Corp. Bradshaw argues its NetIQ Access Manager provides simpler single sign-on capabilities than Workplace Join. That's because Workplace Join requires Active Directory Federation Services, "which is a nightmare to use," Bradshaw says. "NetIQ Access Manage also doesn't need to bother with the management of Group Policies."

ManageEngine, which supplies an MDM tool called Desktop Central, also doesn't plan to integrate with Workplace Join, according to Ananth Vaidyanathan, a product marketing manager. "We don't actually integrate with Workplace Join and we don't recommend that," he says. "It is not a mandatory thing to have Workplace Join for managing mobile devices using the product Desktop Central," adding that customers haven't requested Workplace Join integration. But he says if it's necessary in the future the company would provide it. R

Jeffrey Schwartz is editor in chief of Redmond.

Centrify® DELL Software Redmond THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY