Executive Summary

Changes in technology in recent years have increased users’ expectations for being able to connect to corporate resources from wherever users might be—and from an increasing number of devices. Touch features in Windows 8* coupled with energy-saving innovations in 4th generation Intel® Core™ processors and Intel® Atom™ processors have made Windows PCs attractive as mobile devices. Windows 8.1 and Windows Server 2012 R2* introduce a number of new features that help increase user productivity on mobile Windows devices while making mobile management and secure access to corporate resources from non-domain joined devices possible.

This guide walks you through configuring Windows 8.1 and Windows Server 2012 R2 to take advantage of these four new features:

• Workplace Join
• Web Application Proxy
• Work Folders
• Open Mobile Alliance Device Management (OMA DM)

Beyond exploring this new feature set, this paper also provides guidance on configuring Windows Intune* to work with the OMA DM protocol built into Windows 8.1. However, unless coupled with other solutions like Microsoft System Center 2012 Configuration Manager*, Windows Intune cannot take advantage of all of the capabilities of the built-in OMA DM agent. This guide also provides guidance on configuring Windows Intune to serve as a mobile device management (MDM) authority and configuring System Center 2012 Configuration Manager to serve as an MDM authority by means of the Windows Intune connector.

An overview of the test environment used to capture these configuration steps is provided with this guide, in addition to step-by-step guidance.
Introduction

IT has fundamentally shifted in recent years and employees no longer work almost exclusively on corporate-owned Windows PCs joined to an Active Directory Domain Services* (AD DS) domain. Now, many users in an organization expect to be able to connect to corporate resources wherever they are from their Apple iPhone* and iPad* devices and from Android* devices to get work done. Widespread Windows PC support for touch is a recent addition to this mix. Energy-saving innovations in 4th generation Intel Core processors and Intel Atom processors have increased battery life and made PCs more attractive as mobile devices. Fan-less tablets made possible by energy-efficient Intel Core processors and Intel Atom processors have also given workers a truly mobile experience while running a full version of Windows. Enhancements in Windows 8.1 and Windows Server 2012 R2 now offer the possibility of a different management model for Windows 8.1 PCs. For the first time, it's possible to manage Windows 8.1 clients through enterprise mobility management software instead of through traditional methods.

Traditional client management begins when a client PC receives a corporate image and is joined to AD DS. IT centrally manages each user's operating system and all settings, applications, drivers, and patches on the client. AD DS allows you to centrally manage these client computer software installations and configuration settings through tools such as Group Policy, System Center, or Windows Server Update Services (WSUS). The biggest benefit of traditional management is the high degree of control, stability, and security that you can bring to each user's environment. On the downside, it can be very resource-intensive and can present users with unwanted intrusions by IT onto personal mobile devices.

Enterprise mobility management is a lighter-touch administration style that still gives you a certain amount of control over devices' configuration settings, applications, and data. It enables non-domain-joined devices to have selective access to corporate resources depending on the amount of control IT has over the devices (and depending on IT's risk tolerance). This management alternative is often used to allow employees to access workplace resources from their personal devices, but it can be used to support company-owned devices as well. Currently, Windows Intune and AirWatch support Windows 8.1. Other solutions will offer support in the near future.

There are some good reasons not to join devices running Windows—such as tablets, 2 in 1 devices, or Ultrabook™ devices—to a corporate domain, even when you can. The bring-your-own-device (BYOD) scenario provides the most obvious example: if users bring their own personal mobile devices to work, the very suggestion of joining AD DS can be a non-starter. Employees naturally can be hesitant to cede control of their personal devices to their employer. Windows 8.1 and Windows Server 2012 R2 make possible mobile management of devices based on Windows. This user guide walks you through many of the steps necessary to configure Windows Server 2012 R2 to take advantage of these new features in Windows 8.1.

Technical Overview

Your users at all levels of business expect to connect their consumer mobile devices to corporate resources from wherever they are. Windows 8.1 provides enhancements that make it easier to manage devices running Windows 8.1 as mobile devices, and it can improve the user experience when accessing resources from outside the corporate domain. Coupled with these enhancements...
are powerful new features in Windows Server 2012 R2 that allow users working on Windows 8.1 devices (and sometimes other devices) secure access to the resources they need—regardless of whether their devices are joined to AD DS.

This guide walks you through configuring Windows 8.1 and Windows Server 2012 R2 to take advantage of these four new features:

- Workplace Join
- Web Application Proxy
- Work Folders
- Open Mobile Alliance Device Management (OMA DM)

Beyond exploring this new feature set, this guide also provides guidance on configuring Windows Intune to work with the OMA DM protocol built into Windows 8.1. This guide also provides guidance on configuring Windows Intune to serve as an MDM authority and configuring System Center 2012 Configuration Manager to serve as an MDM authority by means of the Windows Intune connector.

**Workplace Join**

Think of Workplace Join as a state between being fully joined to a domain and not joined at all. With Workplace Join, a user can join a device to the workplace, associating that device with the user and registering a new device object in AD DS, but without gaining all of the network access reserved for fully domain-joined computers. This provides a means of giving your users easy access to both their personal and work-related data from anywhere on their own Windows and iOS* devices while giving you an extra level of security.

When users join a device to a workplace, they install a trusted certificate on the device, securing access and authenticating the user in the future. In Windows 8.1, users can find the Workplace Join option in their PC settings. In the Workplace settings area, they join the device to the workplace simply by entering their domain credentials in the form of an e-mail address and password. (Specifics for joining iOS through Workplace Join are provided in the appendix.)

Workplace Join is also a means of enrolling mobile devices with third-party MDM solutions, such as AirWatch, Mobile Iron, and Windows Intune. Within Windows, a workplace-joined device is registered with IT, but you as an IT administrator do not have control of the device, as you would with a domain-joined PC. The join procedure requires an AD DS user account but not a computer account.

Benefits of Workplace Join include:

- Single sign-on (SSO) to workplace resources and applications
- Streamlined device enrollment with MDM software
- Dynamic access control to resources based on the user’s identity, the device they are using, and their location
- User access to file-based resources that require a user logon
- A built-in form of second-factor authentication
- The ability to require users to verify their identities through phone calls in order to join devices to the workplace (note: this requires System Center 2012 R2 Configuration Manager)

Workplace Join relies on Windows Server 2012 R2, Active Directory Federation Services (AD FS), Active Directory Certificate Services (AD CS), and AD DS.

**Work Folders**

Besides expecting to work anywhere on any device, users today also expect to be able to work on multiple devices and to have their work saved and synchronized locally across these devices. For example, a CEO might begin the week on the company premises by using a domain-joined PC to edit a document. The main copy of this document might be on a network share, but the file is also synchronized and stored on the local PC. The next day the CEO might fly to Asia for business and need to access the same file locally on her personal tablet during the flight. The following week, she might want to return to her work PC and see all the updates that were made on her business trip the week before automatically synchronized.

As an IT professional, you need to provide users ease of access to their files across devices, but you also need to do so in a secure way. You need to reduce the possibility that sensitive files spread out over multiple devices can be accessed by others if the user loses one of these devices. You need some central control.

Work Folders is a new optional component of the file server role in Windows Server 2012 R2 that efficiently answers the need for secure synchronization of personal or work documents across multiple devices. With Work Folders, a personal user folder stored on a company file server is synchronized to a specific...
location on other external devices. For now, Work Folders are supported only on Windows 8.1 and Windows 8.1 RT devices, but Microsoft has stated plans to support other Windows clients, Apple iPad devices, and Android devices in the future.

Work Folders rely on special shares (referred to as “sync shares”) that you can set up on file servers. When you set up a sync share, you establish a device policy in which you can enforce any or all of three security mechanisms:

- **Limit access to registered devices:** This option requires devices synching to the Work Folder to be Workplace Joined, which in turn opens up the possibility for conditional access to the work folder.

- **Apply encryption:** This option requires that the files synchronized to a device be encrypted through Encrypting File System (EFS) on that device, a process accelerated through Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). The key used for encryption in this case is associated with the enterprise domain. When Work Folders are used with management software such as Windows Intune, access to the data can be revoked by wiping the key, preventing the encrypted data associated with the domain from being unencrypted if the device is lost or stolen.

- **Require password and screen lock:** This option requires the user to log back on to the device after it is left idle.

In addition to the security features that are enforceable when you create the sync share, you can also apply all of the same management and security policies to the share that you can with other folders in Windows Server 2012. For example, you can use File Server Resource Manager to apply quotas, assign file classification attributes to be used with conditional access, or apply Rights Management Services (RMS) protection to help ensure that the files remain encrypted even if they are copied and removed from the device.

**Web Application Proxy**

Users need access to more than just company data. They also need access to their company’s internal web applications, such as line-of-business (LOB) applications. Providing simple, secure access to these applications from any device and from any location can be a huge IT challenge.

Web Application Proxy is a new feature in Windows Server 2012 R2 that simplifies the process of making internal web applications available to authorized users on any device outside the corporate network. The feature is installed as a Remote Access role service in Windows Server 2012 R2. The server on which this role service is installed is placed in a secure location accessible from the Internet.

Unlike a VPN, Web Application Proxy allows selective access to internal web-based applications. The process of making a select web application available to external users is known as “publishing.” Users from outside the company enter the published web application URL in a browser and are directed to the Web Application Proxy at the edge of the company network. If the published web application has been configured to require pre-authentication through AD FS, the Web Application Proxy requires users to enter their credentials at the network edge. Otherwise, the Web Application Proxy simply forwards the request directly to the application server for authentication. In either case, depending on the users’ access permissions, users are then granted or denied access to the desired web applications located within the corporate network.

Web Application Proxy provides the following additional benefits:

- **Web Application Proxy provides access to web applications from any device with a browser (not just devices based on Windows).**
- **IT can control access so that only permitted web applications are visible to each user.**
- **Web Application Proxy can be configured to allow direct access to applications or to forward requests to AD FS for authentication.**
- **Through AD FS, applications published in Web Application Proxy can be configured to require multifactor authentication specifically for registered devices, unregistered devices, devices on the intranet, or external devices.**
- **Users do not need to install any additional software on their devices to access published applications.**
- **Web Application Proxy replaces the AD FS proxy (Federation Service Proxy role service) available in previous versions of Windows Server. This means that Web Application Proxy listens to AD FS requests from the Internet and forwards those requests to an internal AD FS server.**

**Open MDM**

Firms that manage mobile and BYOD devices using third-party MDM solutions can manage Windows 8.1 devices the same way. Windows 8.1 provides built-in MDM client capabilities compatible with the industry-standard OMA DM protocol. This means that users will be able to perform self-service registration out of the box and IT will be able to monitor and manage Windows 8.1 devices with MDM solutions.
The built-in OMA DM–compatible client provides programmatic hooks to allow MDM software to manage many Windows 8.1 client settings. For example, the OMA DM client in Windows 8.1 supports provisioning VPN profiles, wireless networks, certificates, and Work Folders.

Architectural Overview of a Sample Environment

The following sections provide step-by-step guidance for configuring Workplace Join, Web Application Proxy, Work Folders, and Windows Intune to work with a mobile device running Windows 8.1. Note that names and IPs used in this guide are for reference only. Feel free to substitute these values with your own, but remember to track the correlation with the values used here.

- Starting server infrastructure:
  - DC.prowesslabs.com
    - Installed roles and services: AD DS (prowesslabs.com)
    - AD CS (Authority name: prowesslabs-DC-CA)
    - Domain Name System (DNS)
    - Networks: internal—172.16.0.2
    - Startup RAM: 2 GB (dynamic)
  - FS.prowesslabs.com
    - Installed roles and services: AD CS (Authority name: prowesslabs-DC-CA)
    - Domain Name System (DNS)
    - Networks: internal—172.16.0.2
    - Startup RAM: 2 GB (dynamic)
  - WAP.prowesslabs.com
    - Installed roles and services: N/A
    - Networks: internal—172.16.0.4; external—192.16.1.115 (Dynamic Host Configuration Protocol [DHCP])
    - Startup RAM: 2 GB (dynamic)
  - Web.prowesslabs.com
    - Installed roles and services: N/A
    - Networks: internal—172.16.0.5
    - Startup RAM: 2 GB (dynamic)
  - WF.prowesslabs.com
    - Installed roles and services: N/A
    - Networks: internal—172.16.0.6
    - Startup RAM: 2 GB (dynamic)
  - SCCM.prowesslabs.com
    - Installed roles and services: System Center 2012 R2 Configuration Manager and all required roles and services
    - Networks: internal—172.16.0.7
    - Startup RAM: 2 GB (dynamic)
  - DomainClient1.prowesslabs.com
    - Operating system: Windows 8.1 Pro
    - Networks: internal—172.16.0.100
    - Startup RAM: 2 GB (dynamic)

Technical Notes

This lab was engineered using Hyper-V* virtual machines running on a Windows Server 2012 architecture. The guest operating systems include Windows Server 2012, Windows Server 2012 R2, and Windows 8.1. Virtual machines were configured to use an internal virtual network for domain traffic and an external network for Internet access and remote user connectivity testing. This document assumes most of the environment configuration has been completed as outlined above.

This lab used Windows Intune to provide mobile device management through the OMA DM agent built into Windows 8.1. For a more complete discussion of the capabilities and limitations of Windows Intune in this regard, see “Appendix B: Windows Intune OMA DM Protocol Support”

Important: The steps presented in this guide are presented for testing and instructional purposes only and are not production-ready as they are. You will need to tailor the guidance provided in this manual to fit your specific environment. Such customization includes server names and IP addresses but also extends to existing server roles and other aspects of your IT environment.
Deploy Mobile Management Features

Configure the Domain Controller and Certificate Authority for Workplace Join

Before doing anything else, you will need to perform a number of tasks on the domain controller and certificate authority server:

- Create a Group Managed Service Account called “FsGmsa.”
- Create domain user accounts for testing access.
- Grant the AD FS server access to the Web Server certificate template.

1. Create a Group Managed Service Account called “FsGmsa”:
   a. Log on to the domain controller (DC.prowesslabs.com) as a domain administrator.
   b. Open a Windows PowerShell* prompt as an administrator.
   c. Type `Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)` and then press Enter.
   d. Type `New-ADServiceAccount FsGmsa -DNSHostName fs.prowesslabs.com -ServicePrincipalNames http/fs.prowesslabs.com` and then press Enter.

2. Create domain user accounts for testing access:
   a. While logged on to the domain controller, open the Active Directory Users and Computers console.
   b. Create a security group named Employees.
   c. Create two or three accounts that you can use to test access, such as:
      i. Jeff Harris; user name: Harris; password: Pass@word1; group: Employees
      ii. David Jeppesen; user name: Jeppesen; password: Pass@word1; group: Employees
      iii. Double-click each of the user accounts you created and assign each account an e-mail address in the E-mail field. For example, harris@prowesslabs.com.

3. Grant the AD FS server access to the Web Server certificate template:
   a. While logged on to the domain controller, open the Certificate Authority console.
   b. In the left navigation pane, expand the certificate authority for your domain controller (for example, prowesslabs-DC-CA).
   c. Right-click Certificate Templates, and then click Manage.
d. Scroll down in the center pane, right-click **Web Server**, and then click **Properties**.

e. Click the **Security** tab.

f. Click **Add**.

g. In the **Select Users, Computers, Services Accounts, or Groups** window, click **Object Types**.

h. Select **Computers**, and then click **OK**.

i. In the **Enter the object names to select** field type `FS$`, and then click **Check Names**.

j. When the name resolves, click **OK**.

k. In the **Group or user names** list click to select `FS$`.

l. In the **Permissions** pane, select **Enroll** in the **Allow** column, and then click **OK**.

m. Close the Certificate Templates console.

4. Create additional DNS records for device registration:

a. Open the DNS console.

b. Expand **DC** and **Forward Lookup Zones**.

c. Right-click your domain (for example, prowesslabs.com) and select **New Alias (CNAME)**.

d. In the **Alias name** field, type `enterpriseregistration`.

e. In the **Fully qualified domain name (FQDN)** field, type the name of your federation server (for example, `fs.prowesslabs.com`), and then click **OK**.
Install and Configure AD FS for Workplace Join

Now you will install the server certificate to be used by the server, before installing and configuring the AD FS role. Once complete, you will enable device registration by completing the following tasks:

- Request a server certificate.
- Export the certificate for clients and web proxy servers.
- Install and configure the AD FS role.
- Enable the Device Registration service.

1. Request a server certificate:
   a. Log on to the federation server as a domain administrator.
   b. In the Start menu, type `mmc`, and then click the mmc search result.
   c. In the Console1 window, click File, and then click Add/Remove Snap-in.
   d. Select Certificates in the left pane, and then click Add.
   e. Select Computer account, and then click Next.
   f. Leave Local Computer selected, and then click Finish.
   g. Click OK.
   h. In the left navigation pane, expand Certificate (Local Computer).
   i. Right-click Personal and mouse over All Tasks.
   j. Click Request New Certificate.
   k. Click Next on the Before You Begin page.
   l. Leave Active Directory Enrollment Policy selected and click Next.
   m. Check the box for Web Server, and then click More information is required to enroll for this certificate. Click here to configure settings.
   n. On the Subject tab, in the Subject name section, toggle the drop-down menu for Type, and select Common name.
   o. In the Value field beneath Common name, type the name of the federation server (for example, fs.prowesslabs.com), and then click Add.
   p. In the Alternative Name section, toggle the drop-down menu for Type, and select DNS.
   q. In the Value field beneath DNS, type the name of the federation server (for example, fs.prowesslabs.com), and then click Add.
r. In the **Value** field beneath **DNS**, type your enterprise registration alias (for example, `enterpriseregistration.prowesslabs.com`), and then click **Add**.

s. Select the **General** tab.

t. In the **Friendly name** field type the name of your federation server (for example, `fs.prowesslabs.com`).

u. Click the **Private Key** tab.

v. Expand **Key options**.

w. Check the box for **Make private key exportable**, and then click **OK**.

x. On the **Certificate Enrollment** window, click **Enroll**.

y. Click **Finish**.
2. Export the certificate and private key for clients and web proxy servers:
   a. Select Certificates below Personal in the left navigation pane.
   b. Right-click the newly obtained certificate for your federation server (for example, fs.prowesslabs.com).
      Note: Select the certificate for the correct purpose—in this case, Server Authentication.
   c. Mouse-over All tasks, and then click Export.
   d. On the Welcome page, click Next.
   e. Select Yes, export the private key, and then click Next.
   f. Leave the file format details in their default values, and click Next.
   g. Select Password and then provide a password (for example, Pass@word1).
   h. Click Next.
   i. Click Browse to select a location for the certificate export file.
   j. Create a new folder on your target drive (for example, C:) and name it Certificates.
   k. Open your certificates file (for example, C:Certificates).
   l. In the File name field type Federation.pfx, and then click Save.
   m. Click Next, and then click Finish.
   n. Click OK when notified that the export was successful.
3. Install and configure the AD FS server role:
   a. On the federation server, open **Server Manager**.
   b. From the **Dashboard** page, click **Add Roles and Features**.
   c. On the **Before you begin** page, click **Next**.
   d. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
   e. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
   f. On the **Select server roles** page, click **Active Directory Federation Services**, and then click **Next**.
   g. On the **Select features** page, click **Next**.
   h. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
   i. After you verify the information on the **Confirm installation selections** page, click **Install**.
   j. Wait for installation to complete, and then click **Configure the federation service on this server**.
   k. On the **Welcome** page, select **Create the first federation server in a federation server farm**, and then click **Next**.
On the Connect to AD DS page, specify an account with domain administrator permissions for your domain (for example, prowesslabs.com), and then click Next.

On the Specify Service Properties page, use the drop-down menu to select the certificate you previously installed (for example, fs.prowesslabs.com). The federation service name will automatically update to match the name of your certificate.

Provide a display name for your federation service (for example, Prowess Labs), and then click Next.

On the Specify Service Account page, select Use an existing domain user account or group Managed Service Account, and then click Select.

In the Select User or Service Account dialog, type FsGmsa, and then click Check Names. Click OK.

Click Select to specify the FsGmsa account you previously created, and then click Next.

On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database, and then click Next.
s. On the **Review Options** page, verify your configuration selections, and then click **Next**.

**t.** On the **Pre-requisite Checks** page, verify that all pre-requisite checks were successfully completed, and then click **Configure**.

**Note:** You can ignore the warning regarding the Group Managed Service Account.

**u.** On the **Results** page, review the results and whether the configuration has completed successfully, and then click **Close**.

**Note:** We’ve already set the service principal name (SPN) for our service account, and thus this warning can be ignored.

**v.** Close the **Add Roles and Features Wizard**.
4. Enable the Device Registration Service-Ad:

a. Open a new Windows PowerShell prompt as an administrator.

b. Type `Initialize-ADDeviceRegistration`, and then press Enter.

c. When prompted to provide a service account, type your domain name and the FsGmsa account you previously created (for example, `prowesslabs\fsgmsa$`), and then press Enter.

d. Press Y, and then press Enter to confirm. Allow a moment for the operation to complete.

e. Type `Enable-AdfsDeviceRegistration`, and then press Enter. Allow a moment for the operation to complete.

f. Open the AD FS Management console.

g. In the left navigation pane, select Authentication Policies.

h. In the Actions pane, click Edit Global Primary Authentication.

i. Select Enable device authentication, and then click OK.
Install and Configure Web Application Proxy

In this section you will install the Web Application Proxy role to allow you to simulate the experience of a user on a personal Windows 8.1 device using Workplace Join while outside of the corporate domain. To do this, you will:

- Copy and install the Federation Server certificate.
- Install and configure the Web Application Proxy role.
- Publish the Device Registration Web App URL to allow remote Workplace Join.

1. Install the Federation Server certificate:
   a. Log on to your Web Application Proxy server (for example, wap.prowesslabs.com) as a domain administrator.
   b. Create a folder on C: and name it Certificates.
   c. Open Windows Explorer and browse to \FS\C$\Certificates.
   d. Copy the Federation.pfx certificate to C:\Certificates on the Web Application Proxy server.
   e. Right-click Federation.pfx, and then click Install PFX.
   f. On the Welcome to the Certificate Import Wizard page, select Local Machine, and then click Next.
   g. Click Yes if prompted by User Account Control.
   h. Confirm the correct path and file name is specified, and then click Next.
   i. Type the password you specified during export, and then click Next.
   j. Select Place all certificates in the following store, and then click Browse.
   k. Select Personal, and then click OK.
   l. Click Next.
   m. Click Finish to complete the wizard.
   n. Click OK when notified of a successful import.
2. Install and configure the Web Application Proxy role:
   a. On the Web Application Proxy server, open the Server Manager.
   b. From the Dashboard page, click Add Roles and Features.
   c. On the Before you begin page, click Next.
   d. On the Select installation type page, click Role-based or feature-based installation, and then click Next.
   e. On the Select destination server page, click Select a server from the server pool, verify that the target computer is highlighted, and then click Next.
   f. In the Roles list, check the box for Remote Access, and then click Next.
   g. Click Next to skip adding additional features.
   h. Click Next on the Remote Access information page.
   i. In the Role Services list, select Web Application Proxy.
   j. Click Add Features to install the required roles and tools.
   k. Click Next.
   l. Confirm the installation selections, and then click Install. Allow a moment for installation to complete.
   m. Once the installation is finished, click the link for Open the Web Application Proxy Wizard in the Installation progress window.
n. On the Welcome page, click Next.

o. In the Federation service name field, type the name of your federation server (for example, fs.prowesslabs.com).

p. In the User name field, type the account of a domain administrator (for example, prowesslabs\administrator).

q. In the Password field type the password for the account specified, and then click Next.

r. Toggle the drop-down menu to select a certificate to be used by the AD FS proxy and select your federation server (for example, fs.prowesslabs.com).

s. Click Next.

t. Review the Web Application Proxy Windows PowerShell command to be run, and then click Configure.

u. Click Close when configuration completes.

v. Click Close to close the Add Roles and Features Wizard.
3. Publish the Device Registration Web App URL to allow remote Workplace Join:
   b. In the left navigation pane, click Web Application Proxy.
   c. In the Tasks pane, click Publish.
   d. On the Welcome page, click Next.
   e. On the Preauthentication page, select Pass-through, and then click Next.
   f. In the Name field, type Device Registration.
   g. In the External URL field, type https://fs.prowesslabs.com/EnrollmentServer/.
      Note: It is critical to include the / at the end of the URL.
   h. Toggle the External certificate drop-down menu and select your federation server (for example, fs.prowesslabs.com).
   i. Click Next.
   j. On the Confirmation page, click Publish.
   k. Click Close when notified that the web application has been published successfully.
Connect Windows Devices through Workplace Join

In this section, you will connect your Windows device through Workplace Join.

1. Connect Workplace Join in Windows 8.1:

   **Note:** If using a non-domain joined device, you might need to download the certificate authority certificate for your environment in order for Windows to trust the certificates needed for Workplace Join.

   a. Log on to a client device as a domain user.
   
   b. From the bottom right corner, open the Settings menu, and then click Change PC settings.
   
   c. From the left pane, click Network.
   
   d. From the left pane, click Workplace.
   
   e. In the Workplace section, type the e-mail address of your domain account, and then click Join.
   
   f. In the password field, type the password for your domain account, and then click Sign in.
   
   g. Your Windows 8.1 device is now connected to your Workplace.
Install and Configure Work Folders

In order to set up and test Work Folders, you will need to perform a number of tasks on the server intended to host your Work Folders and on a Windows 8.1 client computer joined to your Active Directory domain:

- Create an internal DNS record for Work Folders.
- Install the Work Folders and Internet Information Services (IIS) server roles.
- Install a web server certificate.
- Configure the World Wide Web publishing service.
- Import the Work Folders server certificate on the Web Application Proxy server.
- Configure Web Application Proxy to allow access to Work Folders.
- Configure the Work Folders on a domain-joined client running Windows 8.1.
- Browse to your synchronized Work Folders.

**Important:** This guide assumes that you have a server running Windows Server 2012 R2 with no other roles or features installed and joined to a domain (for example, prowesslabs.com).

1. Create an internal DNS record for Work Folders:
   a. Log on to the domain controller (for example, DC.prowesslabs.com) as a domain administrator.
   b. Open the DNS console.
   c. Expand DC, and then expand Forward Lookup Zones.
   d. Right-click your domain name (for example, prowesslabs.com), and then select New Alias (CNAME).
   e. In the Alias name field, type workfolders.
   f. In the Fully qualified domain name (FQDN) field, type the name of the server that will host the Work Folders (for example, wf.prowesslabs.com), and then click OK.
2. Install the Work Folders and IIS server roles:
   a. Log on to the Work Folders server (for example, WF.prowesslabs.com) as a domain administrator.
   b. Open Server Manager if it does not automatically load.
   c. From the Dashboard page, click Add role and features.
   d. On the Before You Begin page, click Next.
   e. Leave Role-based or feature based installation selected and click Next.
   f. Confirm that your Work Folder server (for example, WF.prowesslabs.com) is selected, and then click Next.
   g. In the Roles list, select Web Server (IIS).
   h. Click Add Features to install the additional required features.
   i. In the Roles list, expand File and Storage Services.
   j. Expand File and iSCSI Services.
   k. Select Work Folders.
   l. Click Add Features to install the required roles and features, and then click Next.
   m. Click Next to skip installing any additional features.
   n. On the Web Server Role information page, click Next.
   o. Click Next to install the default IIS features.
   p. Click Install to complete the role installation.
   q. Once complete, click Close.
3. Install a web server certificate:
   a. On the Work Folders server (for example, WF.prowesslabs.com), open the IIS Manager console.
   b. In the left navigation pane, select the Work Folders server (for example, WF (PROWESSLABS)).
   c. In the center pane, double-click Server Certificates.
   d. In the Actions pane, click Create Domain Certificate.
   e. Fill in the Distinguished Name Properties fields, an example of this is provided below:
      i. Common name: workfolders.prowesslabs.com
      ii. Organization: Prowess Labs
      iii. Organizational unit: Labs
      iv. City/locality: Seattle
      v. State/province: WA
   f. Click Next.
   g. On the Online Certification Authority page, click Select.
   h. Select the Certificate Authority, and then click OK.
      i. In the Friendly Name field, type the server name (for example, workfolders.prowesslabs.com), and then click Finish.
   j. In the Server certificates pane, double-click the workfolders.prowesslabs.com certificate.
k. Switch to the **Details** tab, and click **Copy to File**.

l. Click **Next**.

m. Select **Yes, export the private key**, and then click **Next**.

n. Leave **Personal Information Exchange** selected, and then click **Next**.

o. Select **Password** and supply a password (for example, *Pass@word1*).

p. In the **File name** field type the path to the certificate (for example, *C:\Certificates\WorkFolders.pfx*), and then click **Next**.

q. Click **Finish**, and then click **OK**.

r. Click **OK** to close the **Certificate properties** window.

s. In the left navigation pane, expand **Sites**.

t. Right-click **Default Web Site** and select **Edit Bindings**.

u. Click **Add**.

v. In the **Type** menu, select **https**.

w. In the **SSL Certificate** menu, select the certificate you previously created (for example, *workfolders.prowesslabs.com*), and then click **OK**.

x. Click **Close** to close the IIS Manager console.

4. **Configure the World Wide Web publishing service:**

a. On the Work Folders server, open the **Services.msc** console.

b. Scroll to the bottom and locate the **World Wide Web Publishing Service**.

c. Right-click the **World Wide Web Publishing Service**, and then click **Properties**.

d. In the **Startup type** menu, select **Automatic (Delayed Start)**.

e. Click **OK** to close the service properties window.
5. Configure the Work Folders server role:
   b. Create a folder to contain the synchronized folders (for example, C:\ProwessLabs).
   c. If closed, re-open Server Manager.
   d. In the left navigation plane, click File and Storage Services.
   e. Select Work Folders.
   f. In the Work Folders pane, click To create a sync share for Work Folders, start the New Sync Share Wizard.
   g. On the Before you begin page, click Next.
   h. At the bottom of the Select the server and path page, type or browse to the folder you previously created (for example, C:\ProwessLabs).
   i. Click Next.
   j. Select User alias@domain, and then click Next.
   k. Provide a name for the Windows sync share—the Work Folders—for example, Employee Folders, and then click Next.
l. Click **Add** to grant access to domain users or security groups within your domain (for example, prowesslabs\employees).
m. On the **Specify device policies** page you can require enable additional security if desired. In this case, clear all check boxes, and then click **Next**.
n. Review the **Sync Share** settings, and then click **Create**.
o. Click **Close**.
6. Import the Work Folders server certificate on the Web Application Proxy server:

a. Log on to the Web Application Proxy server (for example, WAP.prowesslabs.com) as a domain administrator.

b. Open Windows Explorer and open the location of your Work Folders certificate (for example, \WF.prowesslabs.com\c$\certificates).

c. Copy the WorkFolders.pfx certificate to C:\Certificates on the WAP server.

d. Right-click WorkFolders.pfx, and then click Install PFX.

e. On the Welcome to the Certificate Import Wizard page, select Store Location Local Machine, and then click Next.

f. Click Yes if prompted by User Account Control.

g. Confirm the correct path and file name is specified and click Next.

h. Type the password specified during export (for example, Pass@word1), and then click Next.

i. Select Place all certificates in the following store, and then click Browse.

j. Select Personal, and then click OK.

k. Click Next.

l. Click Finish to complete the wizard.

m. Click OK when notified of a successful import.
7. Configure Web Application Proxy to allow access to Work Folders:

   
   b. In the Tasks pane, click Publish.
   
   c. On the Welcome page, click Next.
   
   d. On the Preauthentication page, select Pass-through, and then click Next.
   
   e. In the Name field, type Work Folders.
   
   f. In the External URL field, type https://workfolders.prowesslabs.com/sync/1.0/.
   
   g. In the External Certificate menu, select the Work Folders certificate (for example, workfolders.prowesslabs.com).
   
   h. Click Next.
   
   i. Review the Web application settings, and then click Publish.
   
   j. Click Close.
8. Configure the Work Folders on a domain-joined client running Windows 8.1:
   a. Log on to a domain-joined client device as a normal domain user (for example, harris@prowesslabs.com).
   b. Open Control Panel, and then click System and Security.
   c. Click Work Folders.
   d. Click Set up Work Folders.
   e. Type the e-mail address for the user (for example, harris@prowesslabs.com), and then click Next.
   f. Review your Work Folders location, and then click Next.
   g. Select I accept these polices on my PC, and then click Set up Work Folders.
   h. From this section you can review your folder usage and any sync errors that might be occurring.

9. Browse to your synchronized Work Folders:
   a. On the same domain-joined client device, open Windows Explorer.
   b. In the left navigation pane, click This PC.
   c. Under Folders, double-click Work Folders.
Configuring Simple Claims-Aware Web Applications

To test Workplace Join, you will need a claims-aware web application. These next steps will walk you through installing some prerequisite files provided free by Microsoft, and configuring a claims-aware web app. You will:

- Install the IIS server role and supporting features.
- Download and install the Windows Identity Foundation software development kit (SDK).
- Install a Web server certificate.
- Configure the simple claims application.
- Continue website configuration in IIS.
- Configure the claims application to work with the federation server.

1. Install IIS server role and supporting features:
   a. Log on to the Web server as a domain administrator.
   b. In Server Manager, on the Quick Start tab of the Welcome tile on the Dashboard page, click Add roles and features.
   c. On the Before you begin page, click Next.
   d. On the Select installation type page, leave Role-based or feature-based installation selected and click Next.
   e. On the Select destination server page, leave Select a server from the server pool selected and click Next.
   f. On the Select server roles page, select Web Server (IIS), click Add Features, and then click Next.
   g. On the Select features page, select Windows Identity Foundation 3.5, and then click Next.
   h. On the Web Server Role (IIS) page, click Next.
   i. On the Select role services page, select and expand Application Development, select ASP.NET 3.5, click Add Features, and then click Next.
   j. On the Confirm installation selections page, click Specify an alternate source path. Type D:sources\sxs and click OK.
   k. Click Install.

2. Download and install the Windows Identity Foundation SDK:
   b. Click Download.
   c. Select WindowsIdentityFoundation-SDK-3.5.msi, and then click Next.
   d. If notified of a blocked pop-up, click Allow once.
   e. Click Run when prompted to download the MSI file.
   f. Install the SDK accepting all application defaults.

3. Install a Web server certificate:
   a. On the Web server, open the IIS Manager console.
   b. In the left navigation pane, select your Web server (WEB (PROWESSLABS.COM)).
   c. In the center pane, double-click Server Certificates.
   d. In the Actions pane, click Create Domain Certificate.
   e. Fill out in the Distinguished Name Properties fields as follows; an example is provided below:
      i. Common name: web.prowesslabs.com
      ii. Organization: Prowess Labs
      iii. Organizational unit: Computers
      iv. City/locality: Seattle
      v. State/province: WA
   f. Click Next.
   g. Click Select.
   h. Click to select the Certificate Authority, and then click OK.
   i. In the Friendly Name field, type the name of your Web server (for example, web.prowesslabs.com), and then click Finish.
   j. In the Server certificates pane, double-click the certificate you just selected (for example, web.prowesslabs.com).
   k. Switch to the Details tab, and then click Copy to File.
   l. Click Next.
   m. Select Yes, export the private key, and then click Next.
   n. Leave Personal Information Exchange selected and click Next.
   o. Select Password and supply a password (for example, Pass@word1).
   p. In the File name field, type C:\Web Cert.pfx, and then click Next.
   q. Click Finish, and then click OK.
   r. Click OK to close the Certificate properties window.
4. Configure the simple claims application:

a. Copy the contents of `C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Web Application\PassiveRedirectBasedClaimsAwareWebApp` to `C:\inetpub\claimapp`.

b. Edit the `Default.aspx.cs` file so that no claim filtering takes place. This step is performed to ensure that the sample application displays all the claims that are issued by the federation server. Do the following:

   i. Open `Default.aspx.cs` in a text editor.
      
      **Note:** Open Notepad as administrator to edit the `Default.aspx.cs` file.

   ii. Search the file for the second instance of `ExpectedClaims`.

   iii. Comment out the entire IF statement and its braces.
      
      **Note:** Comments are achieved by typing `//` (without the quotes) at the beginning of a line.

   iv. Your FOREACH statement should now look like this:

      ```csharp
      foreach (Claim claim in claimsIdentity.Claims) {
        // Before showing the claims, validate that this is an expected claim.
        // If it is not in the expected claims list then don’t show it.
        // if (ExpectedClaims.Contains(claim.ClaimType)) {
        //   WriteClaim(claim, table);
        // }
      }
      ```

   v. Save and close `Default.aspx.cs`.

c. Open `web.config` in a text editor.

d. Remove the entire `<microsoft.identityModel>` section.

   **Note:** Remove everything starting from and including `<microsoft.identityModel>` up to and including `</microsoft.IdentityModel>`.

e. Save and close `web.config`.

5. Continue website configuration in IIS:

a. On the Web server, switch to IIS Manager.

b. In the left navigation pane, select your Web server (`WEB (Prowesslabs.com)`).

c. Click `Application Pools`, right-click `DefaultAppPool`, and then select `Advanced Settings`.

d. Set `Load User Profile` to `True`, and then click `OK`.

e. Right-click `DefaultAppPool` and select `Basic Settings`. Change the `.NET CLR Version` to `.NET CLR Version v2.0.50727`, and then click `OK`.

f. In the left navigation pane, expand `Sites`.

g. Right-click `Default Web Site` and select `Edit Bindings`.

h. Click `Add`.

i. In the `Type` menu, select `https`.

j. In the `SSL Certificate` menu, select the Web server certificate you previously created (for example, `web.prowesslabs.com`), and then click `OK`.

k. Click `Close` to close the `Site Bindings` window.

l. Right-click `Default Web Site` and select `Add Application`.

m. Set the `alias` to `claimapp` and the `Physical path` to `C:\inetpub\claimapp`.

6. Configure the claims application to work with the federation server:

a. On the Web server, open `Windows Explorer`, browse to `C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5`, and then open `FedUtil.exe`.

   **Note:** Make sure to run `FedUtil.exe` as an administrator.

b. Set the `Application configuration location` to `C:\inetpub\claimapp\web.config` and set the `Application URI` to the URL for your site (for example, `https://web.prowesslabs.com/claimapp/`).

   **Note:** It is critical to include the final `/` in the site address.

c. Click `Next`.

d. Select `Use an existing STS` and browse to your AD FS server’s metadata URL (for example, `https://FS.prowesslabs.com/federationmetadata/2007-06/federationmetadata.xml`).

e. Click `Next`.

f. Select `Disable certificate chain validation`, and then click `Next`.

g. Select `No encryption`, and then click `Next`.

h. On the `Offered claims` page, click `Next`.

i. Select `Schedule a task to perform daily WS-Federation metadata updates`, and then click `Finish`. 
Configuring Your MDM Authority
While both management architectures require the Windows Intune service, using Windows Intune or System Center 2012 Configuration Manager as your MDM authority are mutually exclusive options. If you want to test both methods of managing Windows 8.1 devices through the OMA DM agent, you will need to have the Windows Intune service reset by Windows Intune support before trying the other method. (This process can take two to three business days.)

Configuring Windows Intune* as Your MDM Authority
You can use Windows Intune as a stand-alone cloud-based MDM solution for Windows 8.1 devices. Configuring it to do so requires a number of steps:

- Set Windows Intune as your MDM authority.
- Create users and assign Windows Intune licenses.
- Configure and deploy device policies.
- Assign the MDM authority.
- Configure required DNS records.
- Enroll devices in Windows Intune management.

**Important:** To complete these steps you will need to have first signed up for a Windows Intune trial or purchased a subscription.

1. Set Windows Intune as your MDM authority:
   a. Log on to Windows Intune (https://manage.microsoft.com) using your global administrator account (that is, the account under which you signed up for Windows Intune).
   b. Navigate to the Administration workspace.
   c. Select Mobile Device Management.
   d. In the Tasks menu, click Set Mobile Device Management Authority.
   e. Confirm that you want to set Windows Intune as the Mobile Device Management Authority.

   **Note:** Once you select Windows Intune as your MDM authority, only Windows Intune technical support can undo this choice.
2. Create users and assign Windows Intune licenses:
      **Note:** You will need to log on using the account and password used when Windows Intune was purchased or the trial was registered.
   b. Under Management, click Users.
   c. Click New, and then click User on the Users page.
   d. Complete the wizard to add additional Windows Intune users.
      **Note:** Users must be added to the Windows Intune group in order to access Windows Intune resources. Once added, allow 10-15 minutes for user accounts to provision within Windows Intune.

3. Configure and deploy device policies:
   a. At the top of the Windows Intune Admin page, click Admin Console.
   b. In the left pane, click Policy.
   c. Under Policy, click All Policies.
   d. Click Add.
   e. Under Template Name, select Mobile Device Security Policy.
   f. Under How would you like to use the selected template, select Create and Deploy a Custom Policy, and then click Create Policy.
g. Type a name and description for the new policy.

h. Scroll down to review the policy parameters and configure as it suits your needs.

i. Click **Save Policy**.

j. When prompted to deploy the policy, click **Yes**.

k. Select **All Users**, and then click **Add**.

l. It is recommended to deploy the remaining policy templates as appropriate for your environment.
4. Configure required DNS records:

Clients enrolling in MDM will attempt to connect to "enterpriseenrollment.domain.com." (For example, enterpriseenrollment.prowesslabs.com). This request must be forwarded to the Windows Intune server address.

   a. On the domain controller (DC), open the DNS Manager console.
   b. Expand Forward Lookup Zones.
   c. Right-click the domain name (for example, prowesslabs.com), and then select New Alias (CNAME).
   d. In the Alias name field, type enterpriseenrollment.
   e. In the Fully qualified domain name (FQDN) for target host field, type enterpriseenrollment.manage.microsoft.com, and then click OK.

   Note: If you are using an actual registered Internet domain, you will need to create this DNS record using your domain registrar.

5. Enroll devices in Windows Intune management:

   a. To enroll your Windows 8.1 device as a mobile device (similar to a Windows RT, for example), open the Settings menu and tap Change PC Settings.
   b. Tap Network, and then tap Workplace.
   c. Type your user ID (for example, harris@prowesslabs.com), and then click Turn On.
   d. When prompted, provide your Windows Intune account and password.

   Note: You cannot use different accounts for Workplace Join and Device Management. Once enabled, allow 15–20 minutes for your device to complete registration in Windows Intune.

   Note: To enroll your device as a computer (with an operating system like Windows 8.1 Pro, for example), it is recommended that the Windows Intune client software be installed in place of enabling device management as detailed above.

Configuring Microsoft System Center 2012 Configuration Manager* as Your MDM Authority

Setting System Center 2012 Configuration Manager as the management authority for your mobile environment enables more management options than using Windows Intune on its own. The Windows Intune service is still necessary, but you complete tasks by means of the Windows Intune connector site system role available through the Configuration Manager console.

This section will walk you through setting up System Center 2012 Configuration Manager as your MDM authority, broken up into the following steps:

- Set up Active Directory synchronization.
- Configure your Windows Intune subscription in System Center 2012 Configuration Manager.
- Create and deploy configuration policies.
- Configure company resource access with certificate and VPN profiles.
- Retire mobile devices and wipe corporate data.

Important: This section assumes that you have already completed the following tasks:

- Installed System Center 2012 Configuration Manager
- Configured boundary groups
- Enabled Active Directory user and system discovery
- Purchased an Internet domain
- Configure your domain trust in your on-premises Active Directory if the Internet domain differs from your on-premises domain
- Subscribed to Windows Intune (trial or paid account)
- Not set Windows Intune as your MDM (see "Configuring Windows Intune* as Your MDM Authority")
- Added your Internet domain to your Windows Intune subscription

Do not continue this section until you have completed these prerequisite steps.
1. Set up Active Directory synchronization:
   a. Log on to a domain member server that is not the domain controller as a domain administrator.
   b. If not installed, install the .NET 3.5* and 4 frameworks.
   c. Open Internet Explorer and log on to https://account.manage.microsoft.com using your global administrator account (the account under which you subscribed to Windows Intune).
   d. Under Management, click Users.
   e. On the Users page, locate Active Directory Synchronization, and then click Set up.
   f. Under Active Directory Synchronization, click Activate.
   g. Click Activate again to confirm.
h. Under Install and configure the Directory Synchronization tool, select Windows 64-bit version, and then click Download.

i. Click Run when prompted by Internet Explorer.

j. Click Next on the Windows Azure Active Directory Sync Setup Welcome page.

k. Select I Accept, and then click Next to accept the License Terms.

l. Click Next to accept the default installation path.

m. Wait for the component installation to finish.

n. When complete, click Finish.

o. Ensure Start Configuration Wizard now is selected, and then click Finish.

p. On the Welcome page, click Next.
q. Type the user name and password for the administrator account of your Windows Intune subscription (for example, prowess@prowesslabs.com), and then click **Next**.

r. Type the user name and password for the administrator account of your on-premises Active Directory (for example, administrator@prowesslabs.com), and then click **Next**.

s. Select **Enable Hybrid Deployment**, and then click **Next**.

t. Select **Enable Password Sync**, and then click **Next**.

u. Wait while the configuration finishes.

v. When installation completes, click **Next**.

w. Ensure that **Synchronize your directories now** is selected, and then click **Finish**.

x. Click **OK** when advised to verify Active Directory Synchronization.

y. Return to the Windows Intune **Admin** page in Internet Explorer.

z. Click the **Users** section under **Management** to verify that the Active Directory users are present.
2. Configure your Windows Intune subscription in System Center Configuration Manager:
   a. Log on to the System Center 2012 Configuration Manager server as an administrator.
   b. Open the Configuration Manager console.
   c. In the bottom left corner, click Administration to switch to that workspace.
   d. In the left navigation pane, expand Cloud Services, and then select Windows Intune Subscriptions.
   e. In the Home ribbon, click Add Windows Intune Subscription.
   f. On the Getting started page, click Next.
   g. On the Subscription page, click Sign in.
   h. Check the box to confirm understanding that setting the mobile device management authority cannot be undone, and then click OK.
   i. In the Windows Intune window, provide your Windows Intune administrator credentials (for example, prowess@prowesslabs.com), and then click Sign In.
j. When you return to the Subscription page, click Next.

k. On the Collection page, click Browse to select a user collection to allow device enrollment.

l. Select All Users, and then click OK.

m. In the Company Name field, enter your company name (for example, Prowess), select your Configuration Manager site code, and then click Next.

n. In the Platforms window, select Windows, and then click Next.

o. Skip assigning a code-signing certificate for now and click Next.

p. Provide information for the IT Department (for example, department contact name, phone number, and e-mail address) as desired, and then click Next.

q. Skip customization of the company logo and click Next.

r. Review the settings and click Next.
s. Once the wizard successfully completes the configuration process and adds the connection, click **Close**.

**Note:** This guide will address the warning to add the Windows Intune connector role in the next subsection.

t. In the left navigation pane, expand **Site Configuration**.

u. Select **Servers and Site System Roles**.

v. In the center pane, select the **Primary site server** (for example, `sccm.prowesslabs.com`).

w. Select the **Home** tab, and then click **Add Site System Roles**.

x. Leave the default settings on the **General** page as they are and click **Next**.
y. Skip the configuration of a proxy server and click Next.

z. On the System Role Selection page, select Windows Intune Connector, and then click Next.

aa. On the Summary page, click Next.

ab. When notified that the Roles Wizard has completed successfully, click Close.
3. Create and deploy configuration policies:
   a. Log on to the System Center 2012 Configuration Manager server as a domain administrator.
   b. If closed, reopen the Configuration Manager console.
   c. In the bottom left corner, click Assets and Compliance to switch to that workspace.
   d. In the left navigation pane, expand Compliance Settings, and then select Configuration Items.
   e. From the ribbon menu, click Create Configuration Item.
   f. On the General page, provide a name and description for the new mobile policy (for example, Default Policy).
   g. Toggle the drop-down menu for Select the type of configuration item that you want to create, and then select Mobile device.
   h. Click Next.
   i. Scroll through the available setting groups and select System Security and Windows Server Work Folders.
   j. Select Configure additional settings that are not in the default setting groups, and then click Next.
   k. Toggle the drop-down menu for User Access Control, and then select Always Notify.
   l. Toggle the drop-down menu for Network Firewall, and then select Required.
   m. Toggle the drop-down menu for Updates, and then select Automatic Updates is Required.
   n. Click Next.
   o. In the Work Folders URL field, enter the URL for the Sync Share on your file server (for example, https://workfolders.prowesslabs.com), and then click Next.
p. On the **Additional Settings** page, click **Add**.

q. Scroll to view the built-in configuration items that can be published and enforced on mobile devices.

r. Click **Supported Platforms** in the table header row to sort by platforms.

s. Scroll to see the different platforms that are supported by specific settings.

t. Click **Close**.

u. Click **Next**.
v. On the **Supported Platforms** page, select Windows 8.1, and then click **Next**.

w. Review the platforms that are not supported by the settings specified in this configuration, and then click **Next**.

x. Review the configuration summary, and then click **Next**.

y. When the Create Configuration Item Wizard completes, click **Close**.

z. In the left navigation pane, click **Configuration Baselines**.

aa. From the ribbon menu, click **Create Configuration Baseline**.

ab. In the **Name** field, enter a name for this **Configuration Baseline** (for example, **Default Baseline**).
ac. In the Configuration data section, click Add and select Configuration items from the drop-down menu.

ad. Select the configuration item you previously created (for example, Default Policy), and then click Add.

ae. Click OK to close the Add Configuration Items window.

af. Click OK to complete configuration baseline creation.

ag. In the center pane, select the configuration baseline you previously created (for example, Default Baseline).

ah. From the ribbon menu, select Deploy.

ai. Select Remediate noncompliant rules when supported.

aj. In the Select the collection for this configuration baseline deployment section, click Browse.

ak. Select all users, and then click OK.

al. Change the Simple schedule to run every 10 minutes.

am. Click OK to complete deployment.
4. Configure company resource access with certificate and VPN profiles:

   a. If closed, reopen the Configuration Manager console.
   b. In the bottom left corner, click **Assets and Compliance** to switch to that workspace.
   c. In the left pane, expand **Compliance Settings**, and then expand **Company Resource Access**.
   d. Select **Certificate Profiles**, and then click **Create Certificate Profile** in the ribbon menu.
   e. In the **Name** field, enter a name for the new certificate profile (for example, *ProwessLabs CA*).
   f. Leave **Trusted CA certificate** selected and click **Next**.
   g. On the **Trusted CA Certificate** page, click **Browse** to locate and select your certificate (for example, the previously exported Prowess Labs CA certificate).
   h. Leave the Destination store set to **Computer certificate store – Root**, and then click **Next**.
   i. Select **Windows 8.1** and any other desired platforms, and then click **Next**.
   j. Review the summary and click **Next**.
   k. Once the wizard completes successfully, click **Close**.
l. In the center pane, select the newly created certificate profile, and then click **Deploy** in the ribbon menu.
m. Click **Browse** to select the collection to which to deploy the profile.

n. Select **All Users**, and then click **OK**.
o. Click **OK** to complete the deployment.
p. In the left pane, select **VPN Profiles**.
q. In the ribbon, click **Create VPN Profile**.
r. In the **Name** field, enter the name of your VPN profile (for example, *ProwessLabs VPN*), and then click **Next**.

s. Toggle the **Connection type** drop-down menu, and then select **Microsoft SSL (SSTP)**.

t. In the **Server list** section, click **Add**.

u. In the **Friendly name** field, enter a simple name for the VPN connection (this can be the same as the name of the VPN profile; for example, *ProwessLabs VPN*).

v. In the **IP address or FQDN** field, enter the fully qualified domain name for the VPN connection (for example, *vpn.prowesslabs.com*), and then click **OK**.

w. In the **Connection specific DNS suffix** field, enter the DNS suffix for your domain (for example, *prowesslabs.com*), and then click **Next**.

x. On the **Authentication method** page, click **Next**.

y. Skip adding proxy settings and click **Next**.

z. Skip enabling VPN on-demand and click **Next**.

aa. Select Windows 8.1 and any other desired platforms, and then click **Next**.

ab. Confirm the profile settings, and then click **Next**.

ac. Once the wizard completes successfully, click **Close**.
ad. In the center pane, select the newly created VPN profile, and then click **Deploy** in the ribbon.

ae. **Click Browse** to select a collection to which to deploy the profile.

af. **Click to select All Users**, and then **click OK**.

ag. **Click OK** to complete the deployment.

5. Retire mobile devices and wipe corporate data:
   
   a. **Log on to the System Center 2012 Configuration Manager server as a domain administrator.**
   
   b. **Open the Configuration Manager console.**
   
   c. **In the bottom left corner, click Assets and Compliance to switch to that workspace.**
   
   d. **In the left pane, select Device Collections.**
   
   e. **In the center pane, double-click All Mobile Devices.**
   
   f. **Right-click the device or devices you wish to retire, and then click Retire/Wipe.**
   
   g. **Leave Wipe content and retire the mobile device from Configuration Manager selected, and then click OK.**

   **Note:** Because the device is running Windows 8.1 Pro, a full reset is not possible.

   h. **Click Yes** when asked to confirm retirement of the mobile device.

   **Note:** Now that the device has been marked for retirement, upon its next check-in with the MDM authority, the settings applied will be removed, all certificates will be revoked, and the Work Folders data will be removed. This process can take up to 30 minutes.
Appendix A: Connecting Workplace Join in iOS*
You can also use Workplace Join with mobile devices based on iOS.

1. Connect Workplace Join in iOS:

   Note: You might need to download the certificate authority certificate for your environment in order for your iOS device to trust the certificates needed for Workplace Join.

   a. Open Apple Safari* and browse to the iOS profile page on your federation server (for example, http://FS.prowesslabs.com/enrollmentserver/otaprofile).

   b. When prompted, enter your domain user credentials.

   c. When prompted to install a profile, click Install.

   d. Click Install when prompted to confirm installation.

   e. When installation completes, click Done.

Appendix B: Windows Intune OMA DM Protocol Support
Windows Intune is an evolving product and will gain additional capabilities. As of February 2014, Windows Intune was one of the first MDM solutions on the market to support the OMA DM agent that comes built into Windows 8.1. However, without also coupling it with System Center 2012 Configuration Manager, the capabilities of Windows Intune are rather limited as of the writing of this guide.

Windows Intune Capabilities Using the OMA DM Agent
Users can self-enroll their devices without having to download the Windows Intune desktop client. Self-enrollment is completed through the Workplace Window in Windows 8.1 (from the Windows 8.1 Charms window click Settings, Network, and then Workplace). Users supply their e-mail address (either created by IT in Windows Intune as part of a user account or synchronized to AD DS) and choose whether to self-enroll with Windows Intune, activate Workplace Join on their device, or both.

Once enrolled in Windows Intune, users can access content in the Company Portal, either through a web browser or through the Windows Intune Company Portal App that they can install on the start screen of their device. The Company Portal provides the following capabilities:

- **Viewing IT support and other company information**—Administrators can also publish important information for users (such as contact information for IT support) in the Company Portal to help ensure that they will see the information.

  Administrators can view the following information about devices enrolled in Windows Intune:

  - Manufacturer and model
  - Operating system version
  - Wi-Fi* media access control (MAC) address
  - Total and free storage space available
  - Enrollment date and date/time of last device synchronization with Windows Intune

Windows Intune Limitations Using the OMA DM Agent
Relying solely on the built-in OMA DM agent (that is, without employing additional software solutions or installing the Windows Intune desktop agent on a given device), Windows Intune faces a number of limitations that prevent it from performing some common mobile management tasks, including that it:

- Cannot force installation of software on enrolled devices (including anti-malware products like Microsoft Endpoint Protection*)

- Cannot published desktop software packages (MSI and EXE) to the Company Portal.

- Cannot remotely wipe enrolled devices or user Work Folders

- Cannot install the Windows Intune desktop client from Company Portal

- Cannot show administrators software or software updates installed on a given device

These limitations include only what Windows Intune cannot do without the Windows Intune client installed on a given managed device. This list does not include things that Windows Intune cannot do without also being paired with System Center 2012 R2 Configuration Manager, such as provisioning managed devices with Wi-Fi and VPN profiles.

Microsoft has acknowledged these shortcomings and points out that Windows Intune is an evolving product that will provide additional capabilities in the future. However, Microsoft has not given a timeline for remediating any of these limitations.
Glossary

Active Directory Federation Services (AD FS)—A server role in Windows Server designed to simplify identity federation and provide single sign-on capabilities to end-users accessing applications on the corporate network (see Identity Federation for more information on that topic). Within the context of this guide, AD FS primarily acts as an identity provider, authenticating users to provide security tokens to applications that trust AD FS (as opposed to consuming tokens from other identity providers, another function AD FS can perform). In Windows Server 2012 R2, the provisioning of extranet access to applications and services that are secured by AD FS is no longer provided by an AD FS federation server proxy, but rather by a new Remote Access role service called Web Application Proxy. See Web Application Proxy for more information.

Certificate Server—A server that validates, certifies, and revokes digital certificates used in public-key infrastructures (PKIs) as a means of providing reasonable assurance that individuals accessing network resources are not eavesdropping or using a false identity. This function is provided in the scenario outlined in this guide by the Microsoft Internet Information Services (IIS) server role.

Domain Controller—A server that responds to security requests such as users logging on to a Windows Server domain.

Enterprise Mobility Management (EMM)—Technologies designed to manage mobile devices, wireless networks, and related services that enable the use of mobile computing in the enterprise context. While MDM is a subset of EMM, EMM solutions generally provide security and application management services beyond device management. See Mobile Device Management for more information.

Federation Server—A server providing identity-federation services. In the scenario outlined in this guide, this server role is provided by Active Directory Federation Services (AD FS). See Active Directory Federation Services and Identity Federation for more information.

File Server—A server dedicated to providing shared disk access to users, computers, and devices connecting to a network.

Group Managed Service Account (gMSA)—Managed Windows Server domain accounts that provide to multiple servers automatic password management and simplified management of Service Principal Names (the names by which clients uniquely identify instances of services and allow them to authenticate the accounts running the services). The simplified and automated management functions provided by gMSAs include the delegation of management to other administrators.

Hyper-V—The native hypervisor software that ships with Windows Server 2012 for creating and running virtual machines. See Virtual Machines for more information.

Identity Federation—The linking of user identity attributes stored across multiple, distinct identity-management systems. A widely used subset of federated identity is single sign-on (SSO), in which a given user’s single authentication or token is trusted across multiple identity-management systems or organizations.

Mobile Device Management (MDM)—Software solutions designed to secure, monitor, and manage mobile devices used in a business context. See Enterprise Mobility Management for more information on how MDM differs from broader Enterprise Mobility Management.

Open Mobile Alliance Device Management (OMA DM)—A device management protocol specified by the OMA DM Working Group and the Data Synchronization Working Group. The OMA DM agent that comes with Windows 8.1 enables the native management of devices running Windows 8.1 through third-party MDM products such as those from MobileIron or AirWatch.

Sync Share—Folders storing user files on servers running the Work Folders role in Windows Server 2012 R2. A folder specified to serve as a sync share can already contain user data, which enables the adoption of Work Folders without migrating servers. See Work Folders for more information.

Web Application Proxy—A Remote Access role service in Windows Server 2012 R2 that provides reverse proxy functionality for web applications inside a corporate network. This enables users to access web applications resident inside corporate networks from outside the network on devices of their choosing. Web Application Proxy pre-authenticates access to web applications using AD FS and also functions as an AD FS proxy. See Active Directory Federation Services for more information.

Web Server—A server delivers web content to be accessed from the Internet. In the context of the scenario described in this guide, this content supports enterprise applications.

Work Folders—A server role in Windows Server 2012 R2 that enables users to sync data between their devices and user folders located on a file server located on the corporate network. User devices do not have to be joined to the corporate domain in order to use this feature. See Sync Share for more information.

Workplace Join—A Windows Server 2012 R2 feature that enables administrators to grant more finely delineated access to corporate network resources in a middle ground between no access for non-domain-joined devices and full access for domain-joined ones. Workplace Join grants a degree of governance over devices that might be personally owned without granting full access to the data on the devices.

Virtual Machines—Software-based emulations of the functions and architecture of physical computers. The infrastructure used in creating this guide made extensive use of virtual machines. See Hyper-V for more information.
Not all MDM solutions support Windows 8.1*. Consult with your MDM vendor to see if your MDM solution supports Windows 8.1.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel® may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel’s Web site at www.intel.com.

Copyright © 2014 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.