Enable the Always Offline Mode to Provide Faster Access to Files

13 out of 16 rated this helpful - Rate this topic

Published: April 18, 2012

Updated: July 3, 2013

Applies To: Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2

This document describes how to use the Always Offline mode of Offline Files to provide faster access to cached files and redirected folders. Always Offline also provides lower bandwidth usage because users are always working offline, even when they are connected through a high-speed network connection.

In this document

Prerequisites

To enable the Always Offline mode, your environment must meet the following prerequisites.

- An Active Directory Domain Services (AD DS) domain, with client computers joined to the domain. There are no forest or domain functional-level requirements or schema requirements.
- Client computers running Windows 8.1, Windows 8, Windows Server 2012 R2, or Windows Server 2012. (Client computers running earlier versions of Windows might continue to transition to Online mode on very high-speed network connections.)

- A computer with Group Policy Management installed.

Enabling the Always Offline mode

To enable the Always Offline mode, use Group Policy to enable the **Configure slow-link mode** policy setting and set the latency to **1** (millisecond). Doing so causes client computers running Windows 8 or Windows Server 2012 to automatically use the Always Offline mode.

Note

Computers running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 might continue to transition to the Online mode if the latency of the network connection drops below one millisecond.

To enable the Always Offline Mode

---

1. Open **Group Policy Management**.
2. To optionally create a new Group Policy Object (GPO) for Offline Files settings, right-click the appropriate domain or organizational unit (OU), and then click **Create a GPO in this domain, and link it here**.
3. In the console tree, right-click the GPO for which you want to configure the Offline Files settings and then click **Edit**. The **Group Policy Management Editor** appears.
4. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Network**, and expand **Offline Files**.
5. Right-click **Configure slow-link mode**, and then click **Edit**. The **Configure slow-link mode** window appears.
6. Click **Enabled**.
7. In the **Options** box, click **Show**. The **Show Contents window** appears.
8. In the **Value name** box, specify the file share for which you want to enable Always Offline mode.

9. To enable Always Offline mode on all file shares, type *****.
10. In the **Value** box, type **Latency=1** to set the latency threshold to one millisecond, and then click **OK**.

Note

By default, when in Always Offline mode, Windows synchronizes files in the Offline Files cache in the background every two hours. To change this value, use the **Configure Background Sync** policy setting.

Technology description

Folder Redirection and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location. These features used to be referred to as Intellimirror.

- **Folder Redirection** enables users and administrators to redirect the path of a known folder to a new location, manually or by using Group Policy. The new location can be a folder on the local computer or a directory on a file share. Users interact with files in the redirected folder as if it still existed on the local drive. For example, you can redirect the Documents folder, which is usually stored on a local drive, to a network location. The files in the folder are then available to the user from any computer on the network.

- **Offline Files** makes network files available to a user, even if the network connection to the server is unavailable or slow. When working online, file access performance is at the speed of the network and server. When working offline, files are retrieved from the Offline Files folder at local access speeds. A computer switches to Offline Mode when:

    - The new *Always Offline* mode has been enabled
    - The server is unavailable
    - The network connection is slower than a configurable threshold
    - The user manually switches to Offline Mode by using the **Work offline** button in Windows Explorer

- **Roaming User Profiles** redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers. When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile. Roaming User Profiles is typically enabled on domain accounts by a network administrator.

Want to Setup Offline Files in Windows Server 2012 R2? Well, Offline Files (used for offline folder synchronization) is now called *Work Folders* in Windows Server 2012 R2. To setup Work Folders in Windows Server 2012 R2:

1. Start *Server Manager*
2. Add a new *Role*
3. Add the *File and Storage Services* and *Web Server (IIS)* roles
4. Add the *Work Folders* role service
5. Complete the installation (Next, Next, Finish)
6. You will now need to setup the Work Folders website up with a certificate (I won't go into depth on how to setup a certificate in IIS, but basically, open IIS, go to the Work Folders site, edit the bindings and select https and the associated certificate)
7. In Server Manager, expand *File and Storage Services -> Work Folders*
8. From the Work Folders pane, start the *New Sync Share Wizard* (You might also find this under *Tasks*)
9. Click *Next*
10. Select the server you want to setup your Work Folder *Sync Share* on and either select an existing file share or enter a local path
11. Click *Next* and select an option for which to maintain structure. I recommend choosing the *User alias@domain* format because it's more precise and less prone to conflicts.

Selecting the *User alias* option is useful if you already have a folder structure setup in that format

12. Click *Next*
13. Name the Work Folder and click *Next*
14. Add security groups of users that will require access to the Sync Share.

    Note that if *Disable inherited permissions and grant users exclusive access to their files* is ticked, Administrators won't have access to users Synchronized files. Most companies would deselect this option

15. Click *Next*
16. Set any security options you require and complete the setup of the Work Folders Sync Share
17. Next you will need to setup the clients for Work Folder synchronization. In Windows 8.1 or above, go to the *Control Panel* and select *Work Folders*
18. Click *Set up Work Folders* and go through the wizard
19. Once the setup of Work Folders is complete, there will be an option under *My Computer* called *Work Folders* for users to use

Notes about setting up Work Folders in Windows 2012 R2:

- At the time of writing, Work Folders does not support multi-user access to a single Sync Share. This may be fixed in a future patch
- At the time of writing, Work Folders requires Windows 8.1 or above. There may be a client for previous operating systems in future
- I suspect that in future, Work Folder clients will be able to be set up with Group Policy

Caching

- The caching feature in Shared Folders ensures that users have access to shared files even when they are working offline without access to the network. You can also use Shared Folders or Share and Storage Management to enable BranchCache on shared resources. The BranchCache feature enables computers in a branch office to cache files that are downloaded from a shared folder, and then securely shares the files to other computers in the branch.

Work Folders – Windows Server 2012r2

The popularity of smartphones, tablets, laptops, and other mobile devices has led some companies to adopt a Bring Your Own Device (BYOD) policy, allowing employees to use their personal devices to conduct business and access company resources. However, a BYOD policy can present a lot of challenges:

- The security of a company's data comes into question, as the device can be stolen or lost.

- Storing user data only on the local hard drive of a laptop or tablet is inefficient. For example, you can't control backups, which means that data can be lost if the hard drive stops working.
- Users often have more than one device (e.g., using a laptop and tablet, using a tablet and a smartphone), so it can be hard to keep these devices in sync. As a workaround, users often use Microsoft SkyDrive, Dropbox, Google Drive, or a similar cloud service to store their data and keep their data in sync on all devices they use. However, these services are primarily designed for consumer data, not business data. Users storing business data on any of these services can pose a significant security risk. In addition, administrators can't control the behavior of these services on user's private computers. This makes these services hard and inconvenient to implement in business environments.
- Users who are running mobile computers (e.g., laptops, tablets) that are joined to the company's Active Directory Domain Services (AD DS) domain often need to access company data while they're offline. In Windows Server 2012 and earlier Windows versions, Offline Files are mainly used to keep important data available locally on user's computer, even when the computer isn't connected to the network. However, Offline Files are synchronized only when the user is connected to the company's local network. If the users are offline for a long time, there's a good chance that they're working with old data.

To help overcome these problems, Microsoft has implemented a new technology named Work Folders in Windows Server 2012 R2. This technology enables users to have access to their business data, independent of their location, and enables administrators to control the technology's settings and manage user data.

Work Folders provide access to the latest data, no matter whether the users are located internally or externally. In other words, the Work Folders technology is providing almost same functionality as cloud services, but with one big difference—the work folders are manageable. When using Work Folders, administrators can manage the stored data as well as the users' connections to Work Folders. Administrators can enforce the encryption of Work Folders, control which users can use this functionality, and enforce security settings on the devices that use Work Folders, even if they're not a domain member.

Users can use Work Folders from various types of devices (both domain joined or non-domain joined) while they're in the local network and while they're out of the network (e.g., while at home or traveling). Unlike other technologies with similar purposes in earlier Windows versions, Work Folders can be published to the Internet using the Web Application Proxy functionality (also new to Server 2012 R2), enabling users to synchronize their data whenever they have an Internet connection. To publish Work Folders, you can also use other publishing mechanisms, such as Microsoft Forefront's Unified Access Gateway (UAG). (You can also use Forefront's Threat Management Gateway—TMG—but that mechanism is being deprecated.)

Implementing Work Folders

At the time of this writing, the client support for the Work Folders technology is available only in Windows 8.1 and Windows RT 8.1. However, Microsoft announced plans to make this

technology available for Windows 8, Windows 7, and Apple iOS-based devices such as iPad. There are also some rumors that Google Android-based clients will be supported, but it's still not confirmed. Anyway, this clearly shows that Microsoft is opening AD's doors to other OS platforms, which is definitely beneficial for customers.

To enable Work Folders in your environment, you should have at least one Server 2012 R2 file server and Server 2012 R2 schema updates applied for reasons that'll be explained later. To use Work Folders in full capacity (e.g., using Group Policy to set it up on clients), it's recommended (but not required) to have at least one domain controller (DC) running Server 2012 R2.

It isn't necessary to have the domain functional level raised to Server 2012 to use Work Folders. The Work Folders functionality is actually a subrole of the File and Storage Services role and can easily be installed with Server Manager. It's recommended (but not mandatory) that you also install File Server Resource Manager and the Data Deduplication functionality if you want to manage user data more efficiently. File Server Resource Manager lets you set quotas and file screening policies on users' folders. Data Deduplication, which was introduced Server 2012, lets you optimize disk space usage by writing identical chucks of data only once. You should also consider implementing Active Directory Rights Management Services (AD RMS) or Encrypting File System (EFS) to protect any business-critical files that will be stored in Work Folders.

When you install the Work Folders functionality, the IIS Hostable Web Core and IIS management tools will also be installed. You don't have to configure any IIS settings, but you must assign a trusted SSL certificate to your file server in the IIS console and bind it to port 443 on the default website. The certificate should include the file server's name and the name under which you plan to publish your Work Folders (if these names are different). Make sure that this certificate is trusted by your clients. Trust probably won't be an issue for domain-joined devices, but for the BYOD class of devices, you might need to perform some additional steps (e.g., import the Root CA certificate in the local client's Trusted Root CA store), unless you're using a public certificate from globally trusted Certificate Authority (CA). If you want to use the auto-discover feature, which is discussed later, the SAN name in the certificate must be workfolders.*yourdomainname*, where *yourdomainname* is the DNS name of your domain.

After you install the Work Folders functionality, you need to provision a share where the users' data will be stored. The share can be stored in any location that's accessible by the file server on which you installed Work Folders. When you create the root share, it's recommended that you leave share and NTFS permissions at their default values and that you enable access-based enumeration. When access-based enumeration is enabled, users can only see the folders for which they have access permissions, which is a best practice.

After you create the root share, you can launch the New Sync Share Wizard from Server Manager. (In Server Manager, click File and Storage Services, select Work Folders, and choose New Sync Share from the Tasks menu.) This wizard will walk you through creating the Work Folders structure. After selecting the root folder you provisioned as a share, you need to choose the naming format (user alias or alias@domain) for the subfolders. If you have more than one domain in your AD DS forest, it's recommended that you choose the alias@domain naming format.

You can control access to the Work Folders structure on a per-user or per-group basis, which you configure using the wizard's Sync Access page shown in Figure 1. The users or group must be part of your AD DS domain, which means that although devices can be non-domain joined, users still must have valid Active Directory (AD) credentials. It's recommended that you specify a group for easier management later on. It's also recommended that you disable permission inheritance for the Work Folders so that each user has exclusive access to his or her files.

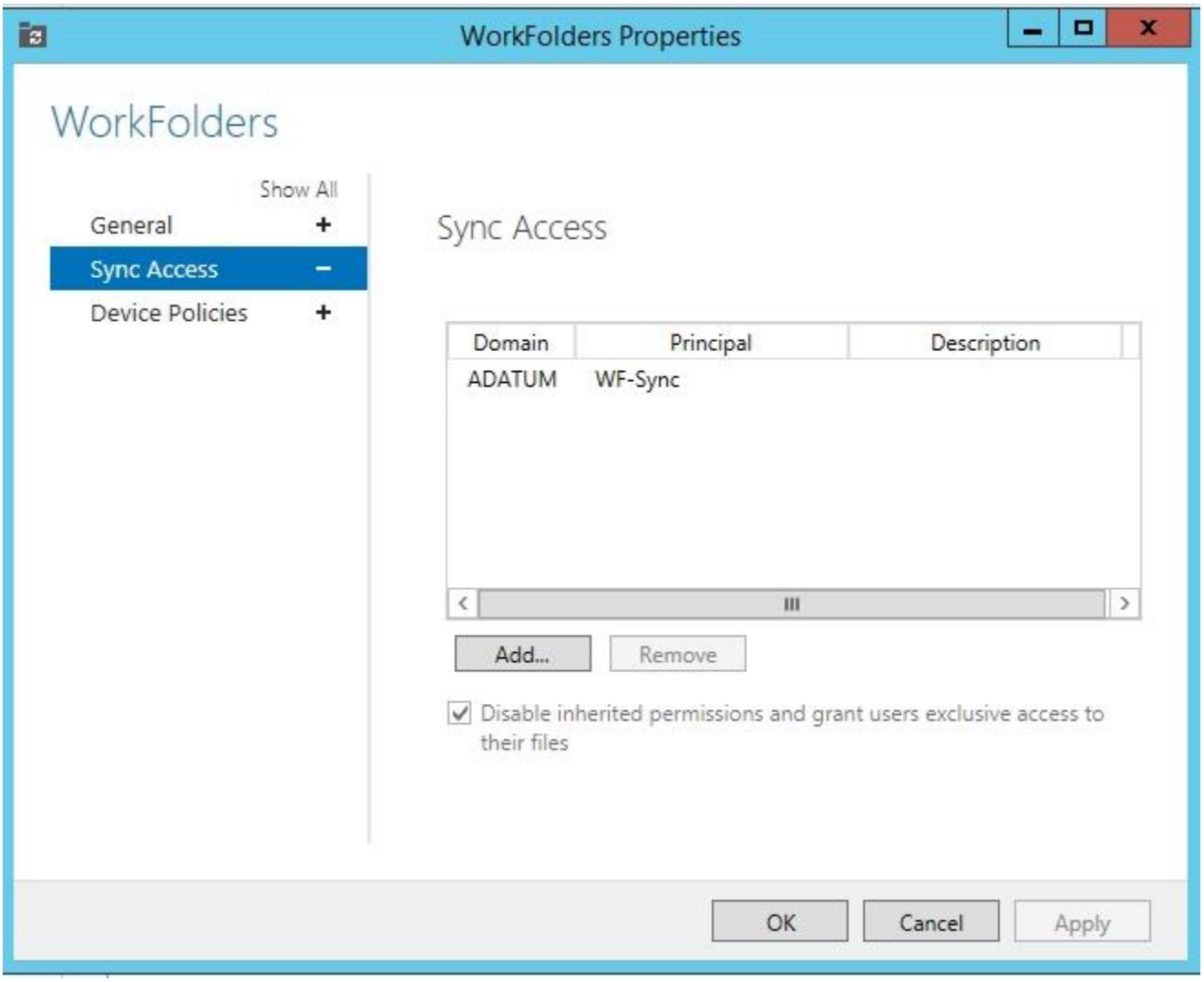

Figure 1: Controlling Access to the Work Folders Structure

On the last page of the wizard, you can configure additional security settings for devices being used to access Work Folders. As Figure 2 shows, you can require encryption and automatically lock screens, which must be unlocked with a password.

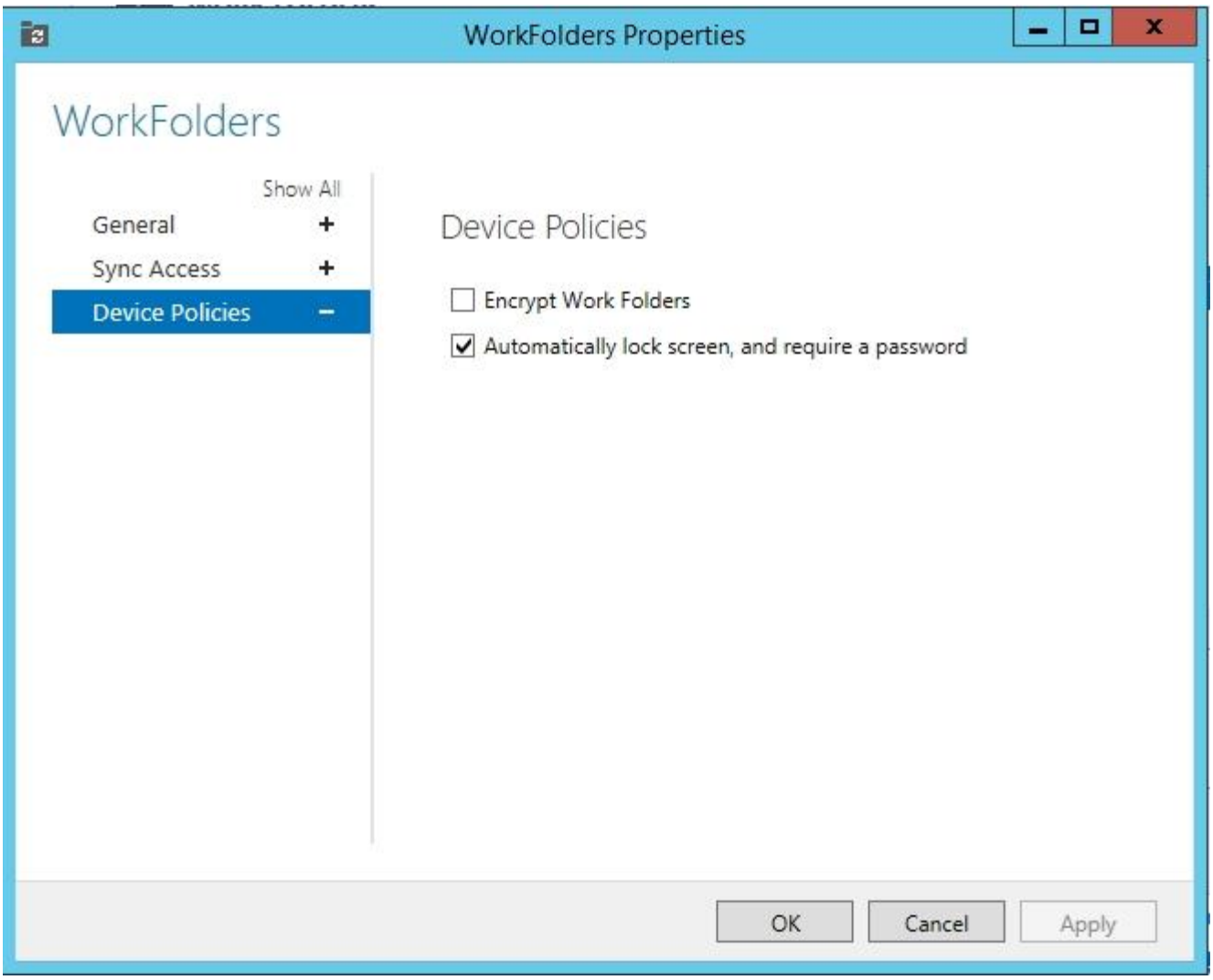

Figure 2: Configuring Additional Security Settings for Devices Being Used to Access Work Folders

It's important to note that the enforcement of security settings related to Work Folders isn't achieved with Group Policy. These settings are enforced when the user establishes a Work Folders connection. They're applied on both computers that are domain joined and on computers that are not domain joined.

Configuring Clients to Use Work Folders

You can configure Windows 8.1 or Windows RT 8.1 clients to use Work Folders manually or automatically with Group Policy. For domain-joined computers, it's easier to configure these settings using Group Policy, but in this case, you must have at least one Server 2012 R2 DC. Non-domain-joined clients must be configured manually. Let's look at both methods as well as what you can do if you have multiple file servers.

Configuring clients with Group Policy. If you want to use Group Policy to automatically configure Work Folders on the clients, there are a few Group Policy Objects (GPOs) settings you need to configure. Work Folders are user based, so you need to navigate to User Configuration\Policies\Administrative Templates\Windows Components\Work Folders in Group Policy Editor (GPE). In the Specify Work Folders settings, enable the policy. In addition, you need to specify the Work Folders URL. This URL is the location of the file server on which you enabled Work Folders. It's usually https://*fileserverFQDN*, where *fileserverFQDN* is your file server's Fully Qualified Domain Name (FQDN).

You also have the option to force automatic setup for each user. This option should be considered with caution. If you enable it, all users to which this GPO applies will have their Work Folders configured on each device they log on to (if the device supports Work Folders), without being prompted to do so. In some scenarios, you might not want to have that outcome. For example, you might not want to use this option if users work on many different workstations.

Optionally, you can also navigate to Computer Configuration\Policies\Administrative Templates\Windows Components\Work Folders in GPE, where you'll find the option to force the automatic setup of Work Folders for all users. Computers that have this GPO setting applied will configure Work Folders for every user that logs on if the user is allowed to use Work Folders.

After you apply these GPO settings to users (and optionally computers), domain users will be able to start using Work Folders once Group Policy is updated or the client computer is restarted. If the Work Folders settings from Group Policy aren't applied, first check the certificate on the file server, as that's the most common cause for problems. Certificates must have a valid name, must be issued by trusted root CA, and must be assigned to port 443 on default website. Also, make sure that the Windows Sync Share service is running on the server where you set up Work Folders. (Although this service is automatically started when you install Work Folders, I've seen cases where it has stopped running.)

Configuring clients manually. If you want to enable Work Folders on a non-domain-joined computer (e.g., a tablet), you need to manually do so in Control Panel. Windows 8.1 and Windows RT 8.1 have a Control Panel applet named Work Folders, as Figure 3 shows.

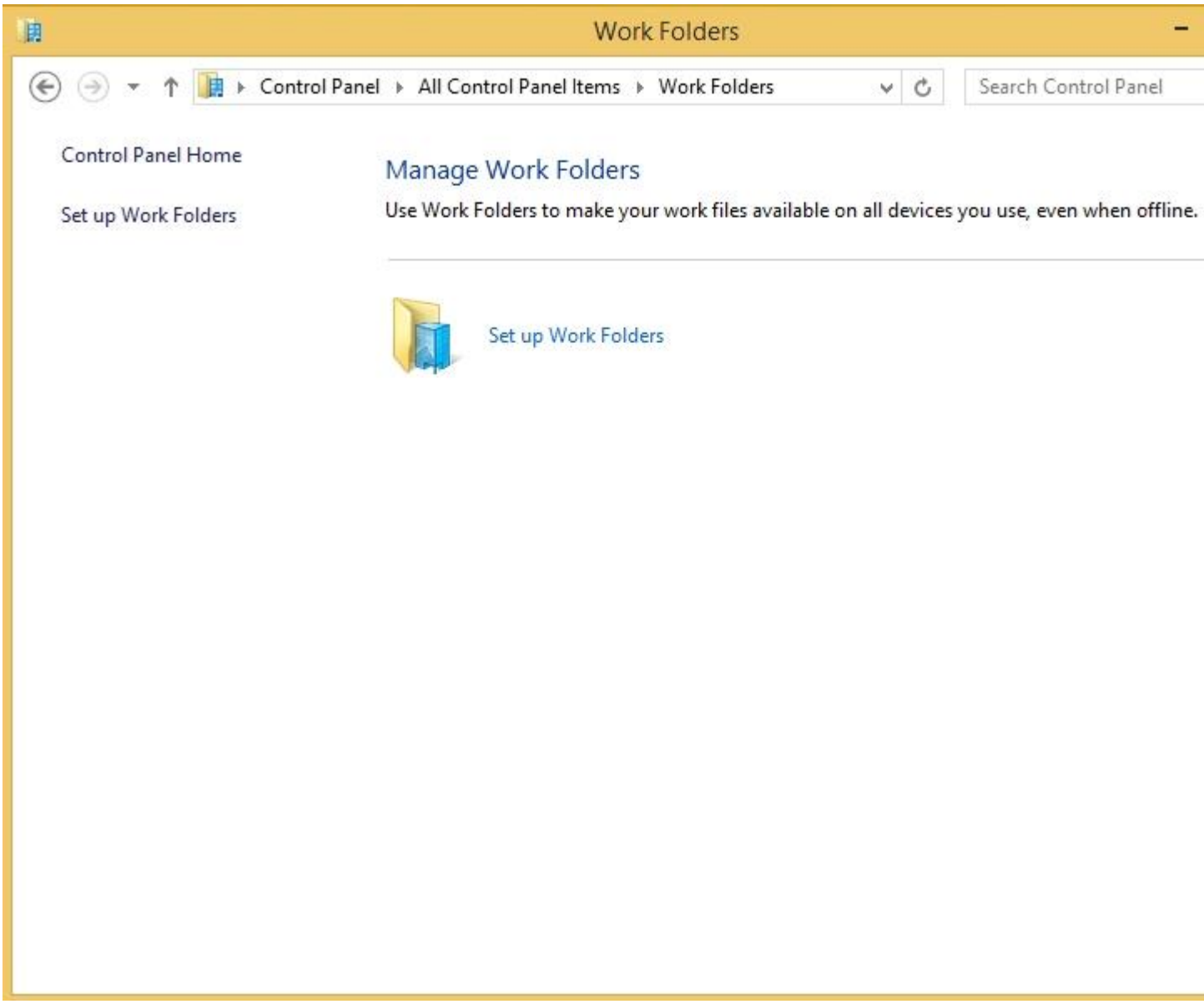

Figure 3: Examining the Control Panel Work Folders Applet

The Work Folders technology has an auto-discover feature that enables non-domain-joined machines to easily locate the proper file server that hosts users' Work Folders. To use this feature, you must have a *workfolders* host or alias in your public DNS that points to the right file server. Once you have this in place, users just need to enter their email address when configuring the Work Folders applet on their non-domain-joined machines. Based on the domain name part of the email address, the machine will search for the workfolders host or alias in the DNS. Users will also need to provide a valid username and password for the domain account that's allowed to use Work Folders.

If you don't want to use the auto-discover feature, you can have the users provide the file server URL when configuring the Work Folders applet on their machines, as Figure 4 shows.

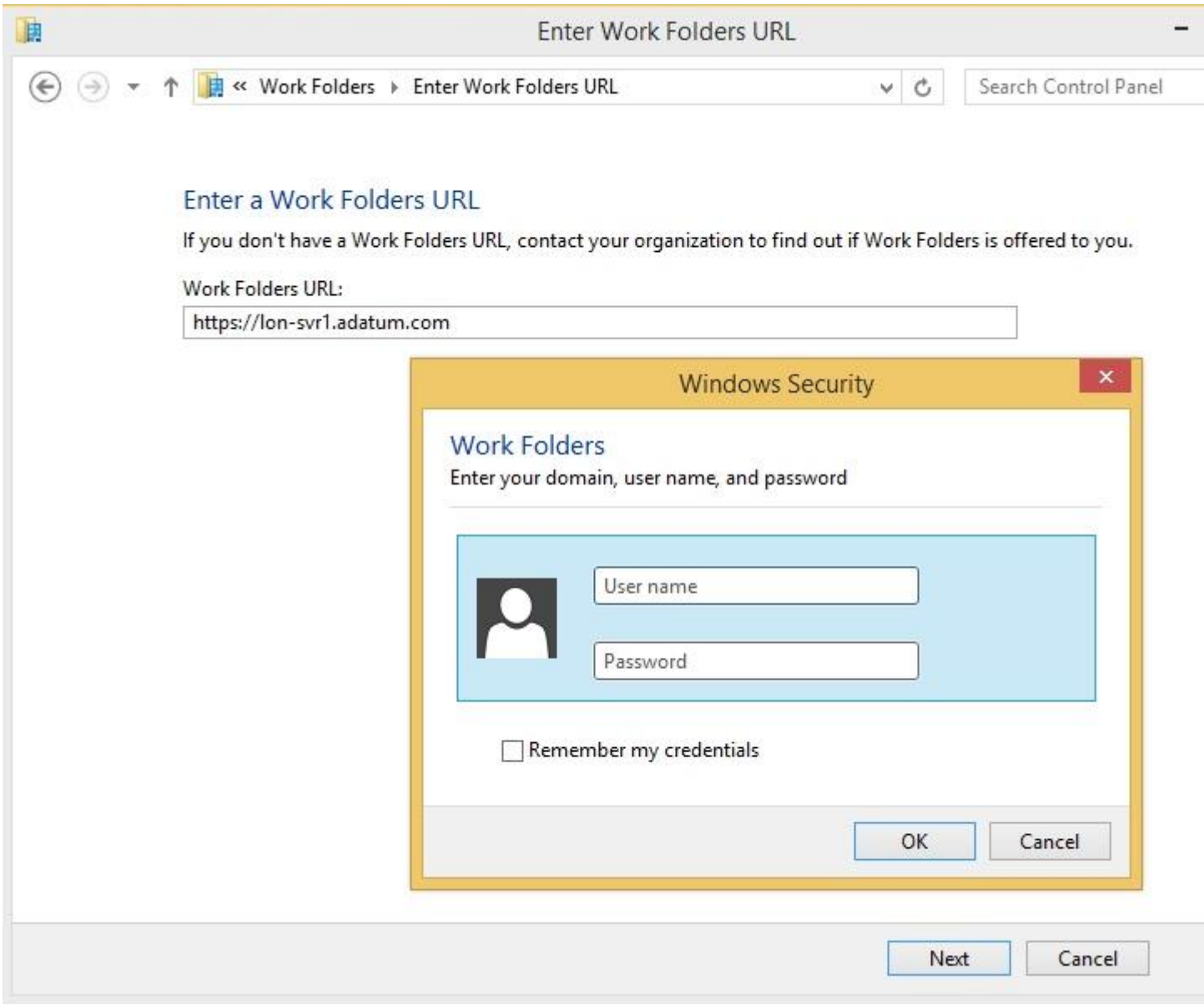

Figure 4: Entering the Work Folders Server URL

In this case, they'll be manually entering the URL that's being used to publish the file server hosting Work Folders to the Internet. If you're not using the auto-discover feature, the URL can be whatever you like. As you can see from the URL example in Figure 4, the connection is being made using HTTP Secure (HTTPS), which makes Work Folders pretty simple for publishing. If the users are logged on as local users, after they provide the URL, they must provide valid AD credentials before the Work Folders functionality is configured on their machines. Also, they must to accept the security policies shown in Figure 5. Basically, the users agree to let the organization's administrator manage the data in their Work Folders and apply security measures to their machines.

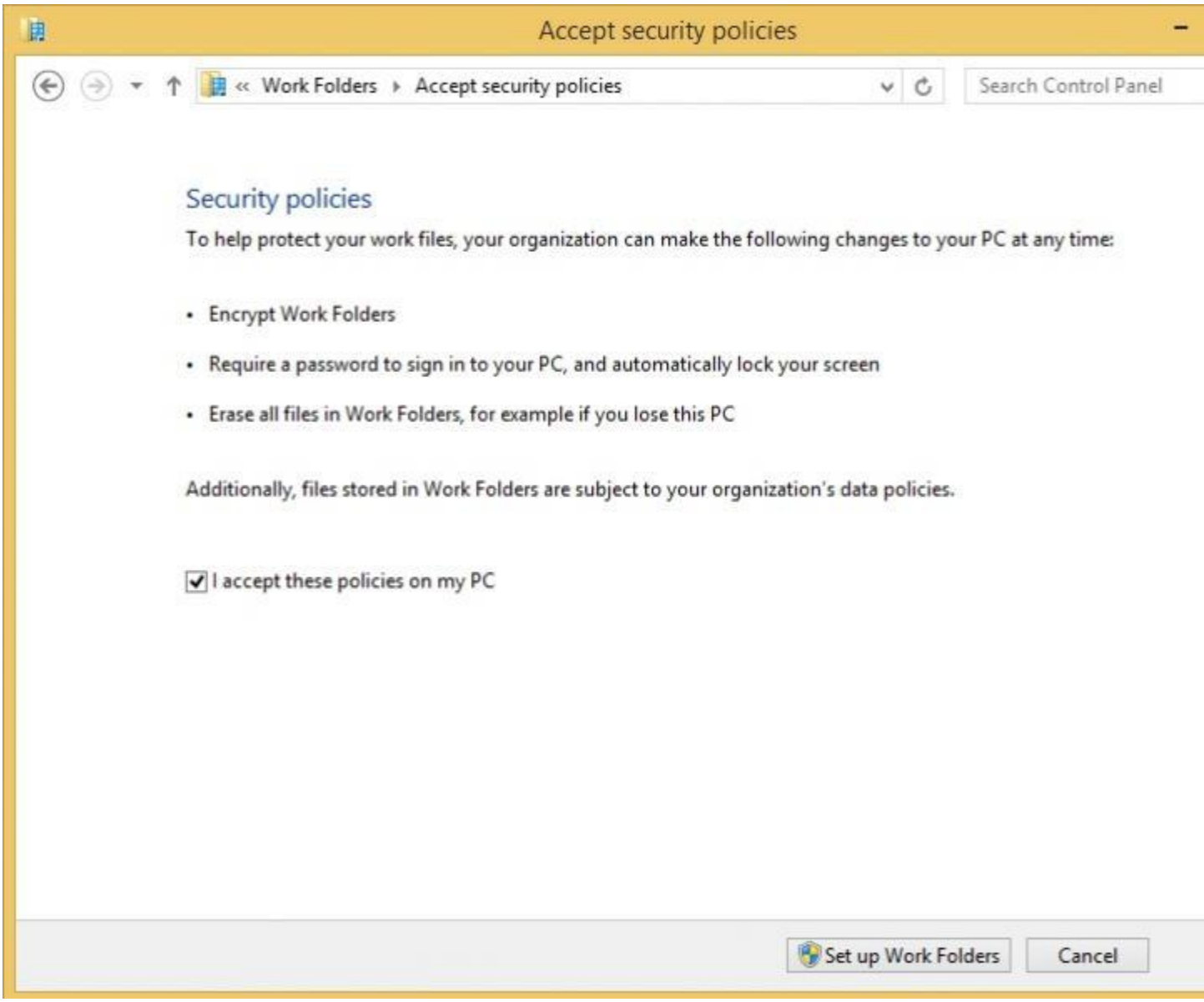

Figure 5: Applying Device Security Policies for Work Folders

Handling multiple file servers. If you have multiple file servers hosting Work Folders, it's good to know that you can configure a new user attribute named msDS-SyncServerUrl in AD DS (it comes with the Server 2012 R2 schema) to specify the proper Work Folders location for each user. You can easily find this attribute on the Attribute Editor tab in User Account Properties. When this attribute is configured, the user will always be directed to the specific file server to locate his or her Work Folder. However, this attribute isn't mandatory in deployment scenarios where only one file server hosts Work Folders or when the Work Folders functionality isn't configured through the auto-discover feature.

Using Work Folders

After the Work Folders settings are applied, users can start using Work Folders, No matter whether they're on domain-joined or non-domain-joined machines, a new icon will appear in File Explorer, as Figure 6 shows. Users work with their Work Folders as they would work with any other folder. The only difference is that when they right-click the Work Folders icon, they have the option to force synchronization with the server. (If the synchronization isn't working, make sure that you have local administrative privileges on client machine so that you can apply security policies from the server.)

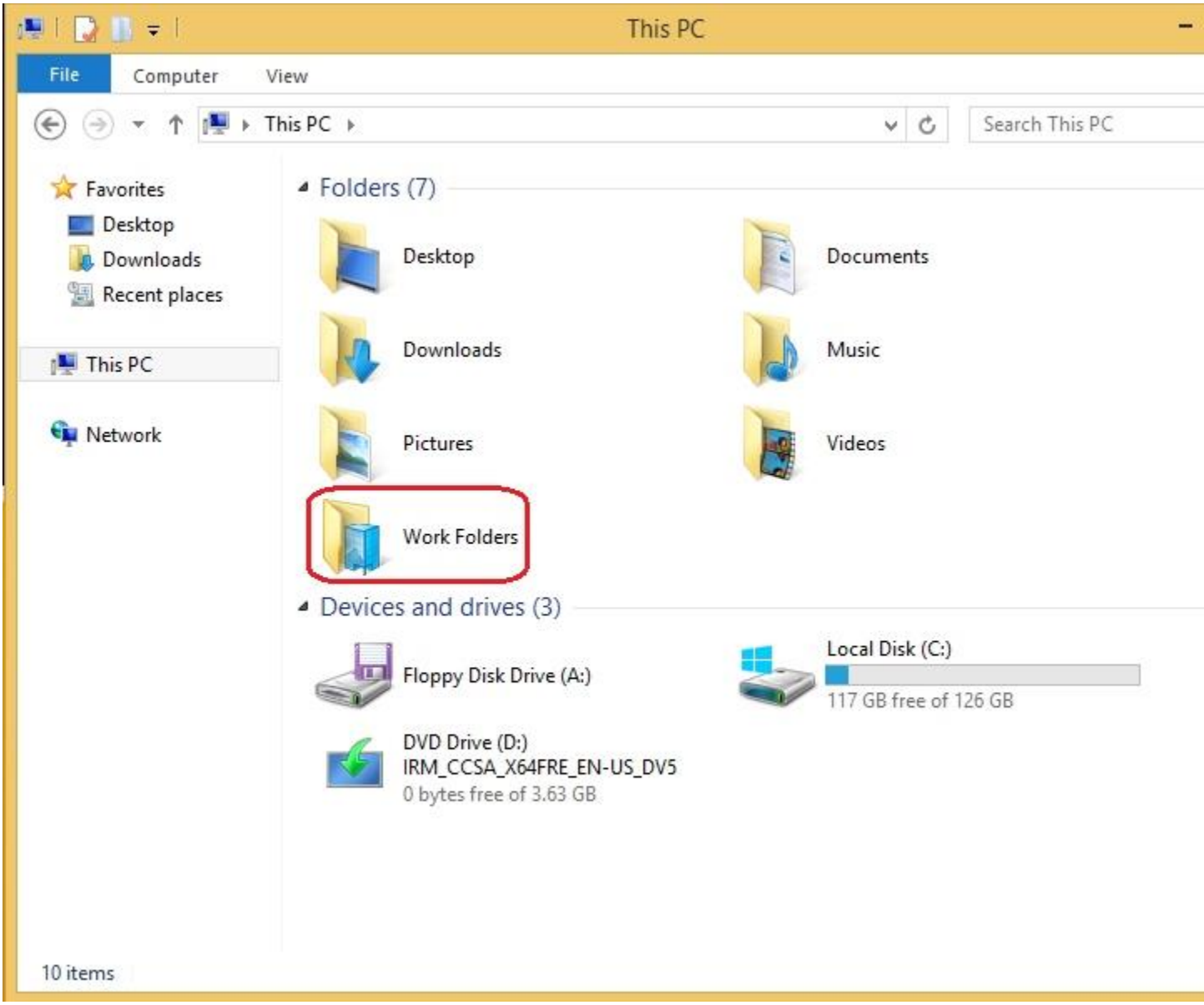

Figure 6: Examining the New Work Folders Icon in File Explorer

If desired, users can monitor the health of their Work Folders in the Work Folders applet, no matter whether they're on domain-joined or non-domain-joined machines. As Figure 7 shows,

they can find out how much space is available on the server and when their files were synchronized last.

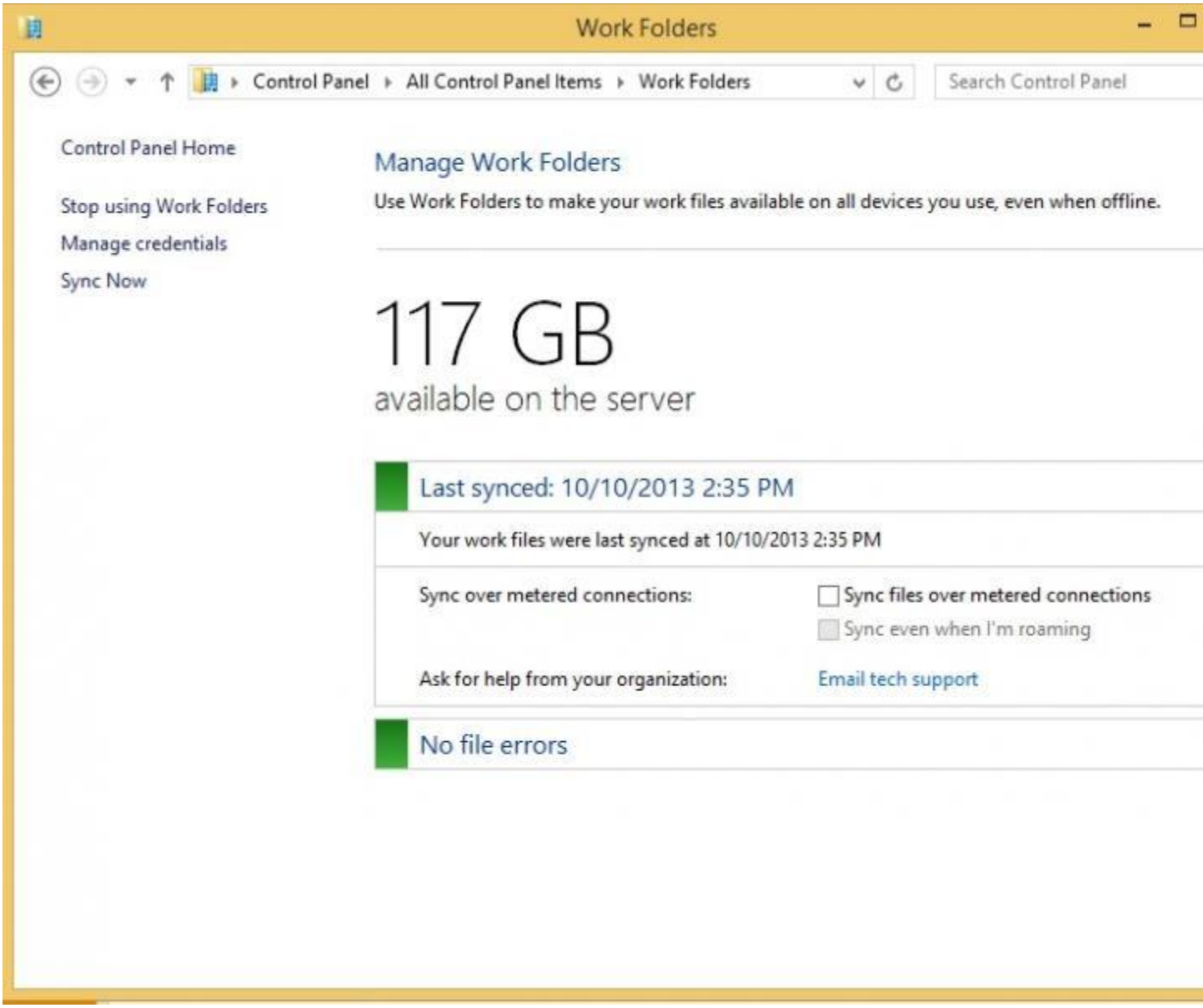

Figure 7: Monitoring the Health of Work Folders in Control Panel

Managing Work Folders

Administrators can manage Work Folders through the Work Folders interface integrated in the Server Manager console. At any time, you can see which users are currently connected to Work Folders, as shown in Figure 8.

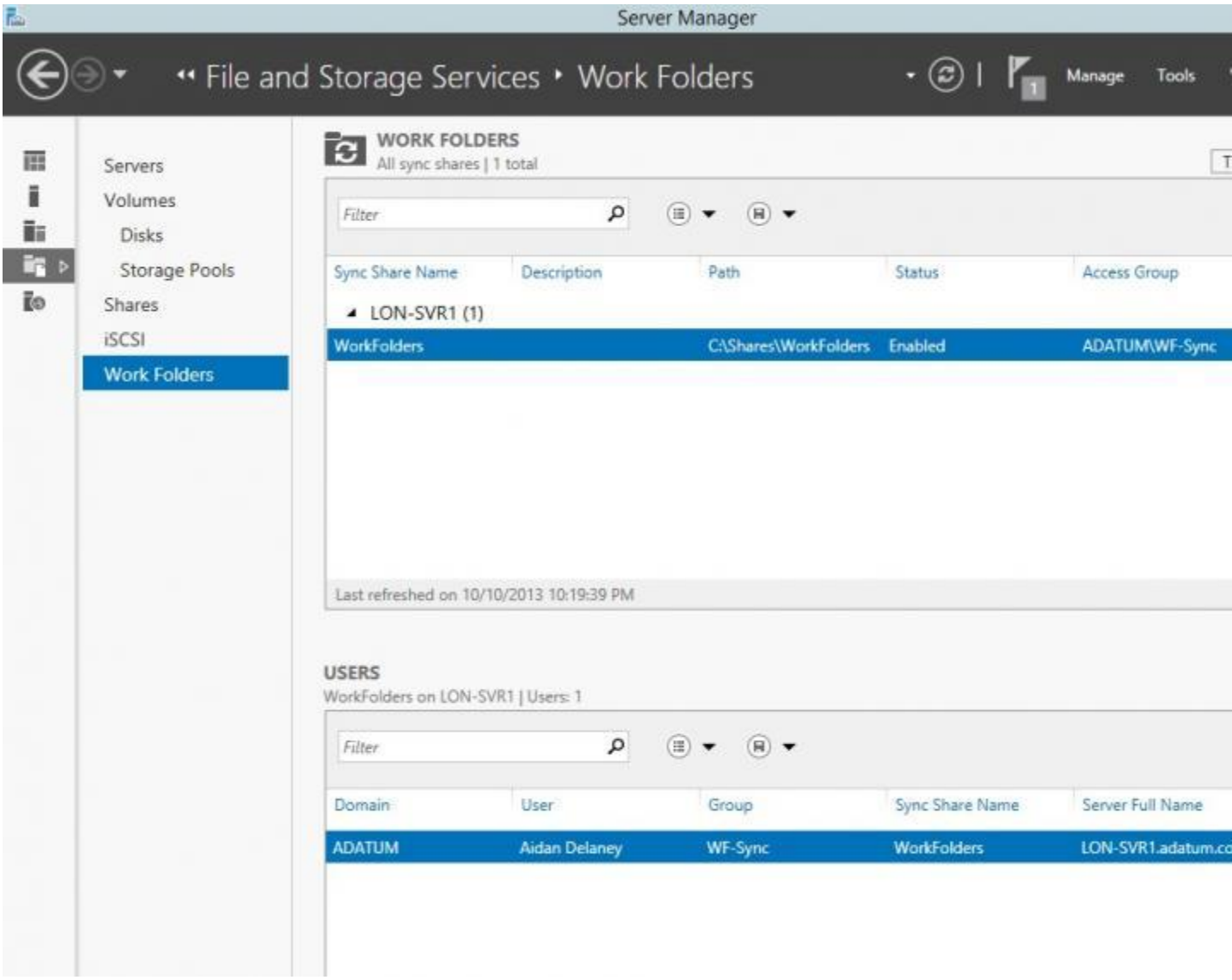

Figure 8: Seeing Which Users Are Currently Connected to Work Folders

Right-clicking a user's name brings up two options—Properties and Suspend User—as seen in Figure 9.

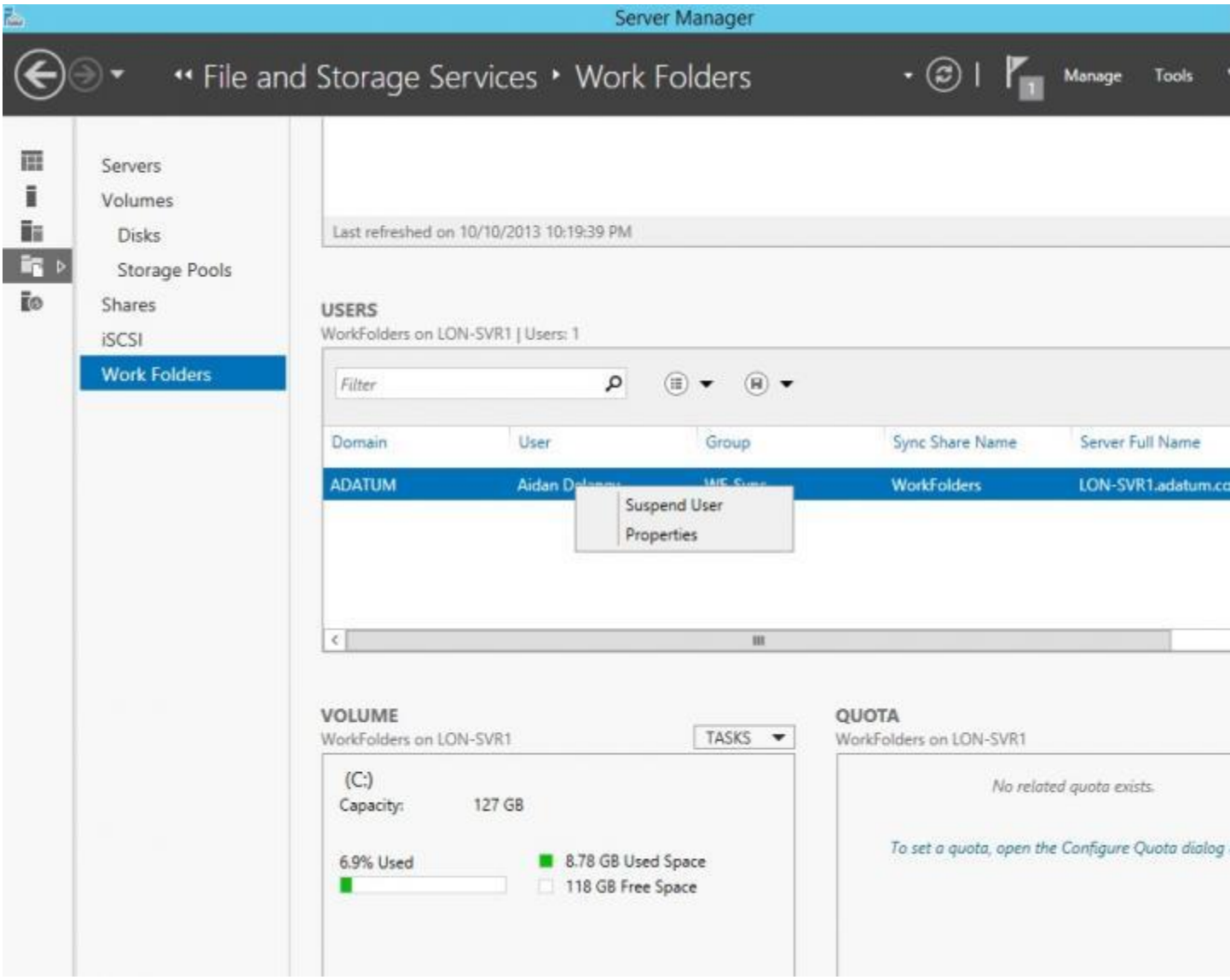

Figure 9: Drilling Down for More Information

If you select the Properties option, you can see how many devices that particular user has associated with his or her Work Folder, as Figure 10 shows. If you select the Suspend User option, you'll stop the synchronization between the user's local Work Folder and the Work Folder on the server. However, user can still access the local copy of the data. You can resume the synchronization by right-clicking the user's name and selecting the option to resume synchronization.

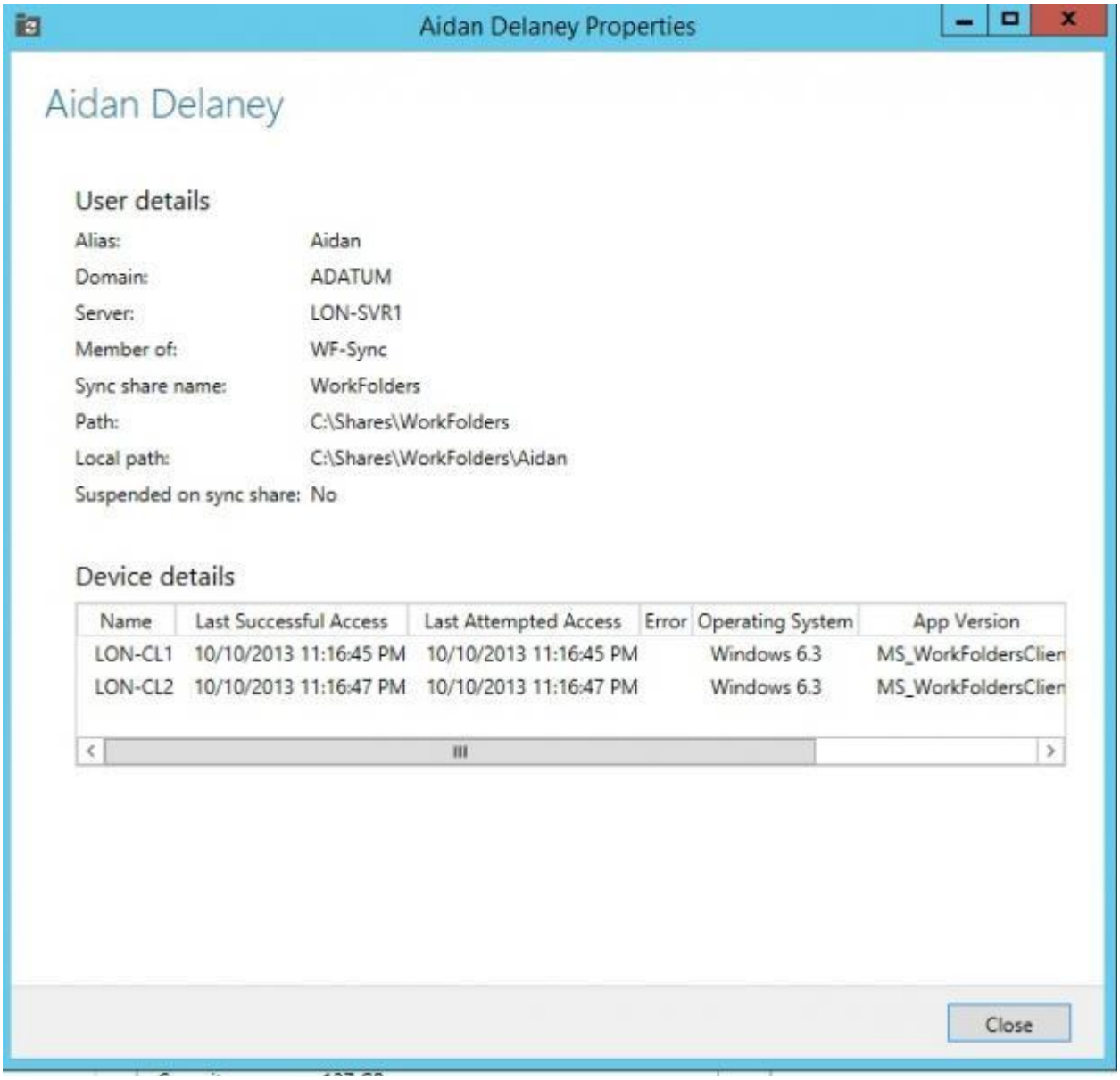

Figure 10: Seeing How Many Devices a User Has Associated with His or Her Work Folder

By default, administrators can't access the server copy of a user's Work Folder, as permissions are automatically set for the owner only. However, if necessary, it's possible to take ownership of the folder and access the data. Each user can access the server copy of his or her data by browsing to the file server location. No other folders are accessible—and if access-based enumeration is enabled, users won't even see any other folders.

A Significant Enhancement

The Work Folders functionality in Server 2012 R2 represents a significant enhancement over current technologies for data synchronization and accessibility. It provides the benefits of cloud-based solutions but still gives administrators the ability to control the technology's settings and manage users' data. Work Folders can be very useful for mobile users, especially in a BYOD

environment. If Microsoft opens this technology to other platforms as promised, Work Folders will greatly help users always keep their data with them.