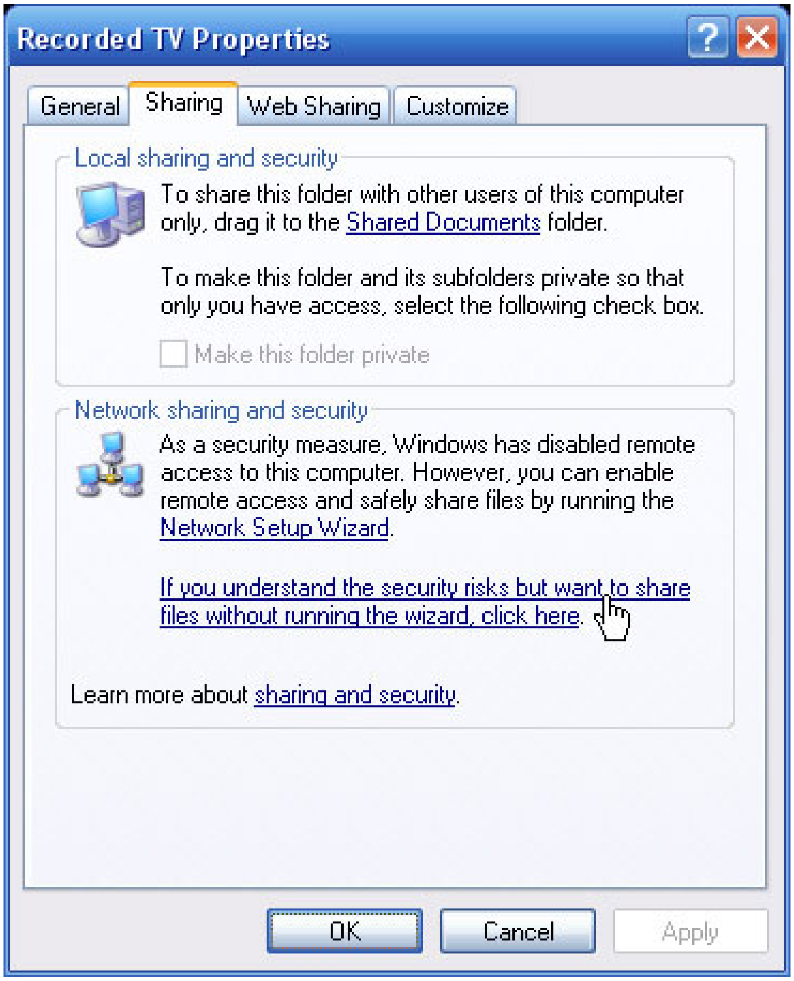
The Old New Thing

Things I've written that have amused other people, Episode 9

1 Feb 2012 7:00 AM 29

A customer liaison reported that their customer wants to be able to access their machine without needing a password. They just want to be able to `net use * \\machine\share` and be able to access the files right away. I guess because passwords are confusing, easy to forget, and just get in the way. Anyway, the customer discovered that they could do so on Windows XP by going to the folder they want to share, going to the Sharing tab, then clicking on the *If you understand the security risks but want to share files without running the wizard* link,



To share this folder with other users of this computer only, drag it to the Shared Documents folder.

To make this folder and its subfolders private so that only you have access, select the following check box.

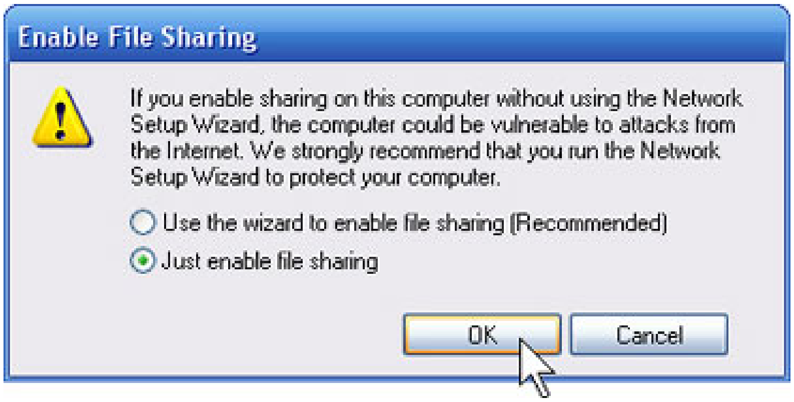
□ Make this folder private

As a security measure, Windows has disabled remote access to this computer. However, you can enable remote access and safely share files by running the Network Setup Wizard.

If you understand the security risks but want to share files without running the wizard, click here.

Learn more about sharing and security.

and then on the *Enable File Sharing* dialog, clicking *Just enable file sharing*.



Enable File Sharing

If you enable sharing on this computer without using the Network Setup Wizard, the computer could be vulnerable to attacks from the Internet. We strongly recommend that you run the Network Setup Wizard to protect your computer.

○ Use the wizard to enable file sharing (Recommended)

● Just enable file sharing

What the customer wanted to know was if there was a way they could automate this process.

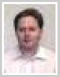
My response to the customer liaison went like this:

> Your customer has chosen to ignore not one but two security warnings. Furthermore, since they are looking for an automated way of doing this, it sounds like they intend on deploying this "feature" to all the computers in their organization. Maybe they just enjoy being part of a botnet? Your customer is basically saying "I wish my computer to have no network security." They should at least restrict access to authenticated users. But if they if they insist on having their corporate network turned into a spam farm, they can enable the Guest account and say that it can "Access this computer from the network." Congratulations, your computers will soon be filled with malware and porn.

That last sentence made it into some people's quotes file.

Blog - Comment List MSDN TechNet

Comments



Maurits [MSFT]

1 Feb 2012 7:06 AM

#

Y U assume they don't have the shared folder locked down with NTFS permissions? I seem to recall at least one book recommending that permissions always be applied at the NTFS level rather than the share level. (Personally I ignored this advice and applied permissions on the share rather than at NTFS.)

John

1 Feb 2012 7:08 AM

#

Should have just told them to turn off automatic updates; the malware coming in on the next remote execution vulnerability would open up their network for them. The best part is that 1) turning off automatic updates can be automated and 2) you only have to ignore one security warning.

GWO
1 Feb 2012 7:51 AM
#

All of which presupposes that the network in question is connected to the Internet with a VPN, DMZ or a strong firewall.

Mc
1 Feb 2012 8:02 AM
#

Ah, but they were going to use a $ in the sharenames and have it secret+secure that way. :-)

george
1 Feb 2012 8:11 AM
#

You signed me when I read the porn part! :D

gm
1 Feb 2012 8:13 AM
#

Understood, but in all honesty, the security model in some Windows versions are so f*cking complicated to the uninitiated, that we are left for hours sometimes just scratching our heads... "Why does it still not work!!!??"

We give up and open the floodgates. Just share any damn file, damn the security. That's when we do stupid ass stuff like this.

My most recent moment of "Why is something so simple so $%^$%# hard to do?" came when one of my computers (all Windows 7) at home refused to join the homegroup. No matter what i did, it still to this day refuses to recognize that there is an existing homegroup. If I create a new homegroup on this computer and then attempt to have the others join the homegroup of this one computer I get the exact same thing: They do not see each other. Yes, I have checked and triple checked they are on the same subnet, same DHCP server, same blah blah blah. Still it does not work. the next option was to reinstall Windows from scratch, and I did not have the time to deal with that mess.

User error/ignorance or not, I just gave up and enabled passwordless sharing, which accomplishing that was another pain in the ass, but at least it worked.

So, in defense of that customer, I will say that the root cause might be something that either did not work as intended, or was too complicated and opening the floodgates seemed like a quicker fix.

gm
1 Feb 2012 8:17 AM
#

Oh and don't get me started on "Troubleshoot this problem" wizards and help files included in Windows... Do you guys measure how often those things actually solve anything?

Seriously, I'd actually be very interested in the stat if MS has it (and if not, why are you guys not measuring it?). It has not helped me once in all my years with Windows, I wonder if troubleshooters and help files are helpful to anyone at all.

Joshua
1 Feb 2012 8:20 AM
#

It would be nice to have the ability to automatically click those items, _and_ disable use of the guest account for remote connections all at once.

Always use guest account is the bane of having secure networking with XP Home.

Martin Bonner
1 Feb 2012 8:31 AM
#

@gm: Those wizards won't help anyone reading Raymond's blog. They are designed to help my sister and maybe my mother (my mother may find them a bit tricky to run).

gm
1 Feb 2012 8:51 AM
#

@Martin: Agreed, but still I've never heard of them helping anyone. And the suggestions in the help files do not make that much sense. Users would be far better off of those help screens were merely shortcuts to web searches for the error code. Unless the problem is with getting networking up and running, which in that case, the help files and troubleshooters simple need to be far better than they are now.

kinokijuf
1 Feb 2012 8:51 AM
#

OMG pictures!

NB

1 Feb 2012 9:15 AM

#

I feel their pain.

(Never quite got comfortable with configuring DCOM between two machines.)

JM

1 Feb 2012 10:00 AM

#

@NB: DCOM just likes playing hard to get. Like a bashful virgin maiden betrothed to another, it knows that attempts to woo it are doomed to end in heartache and ruin, so it wears its many options, toggles, hurdles and dire warnings as a chastity belt.

Gabe

1 Feb 2012 10:24 AM

#

Actually, it sounds like it would be really handy to be able to get all that porn without having to do the work of going out and finding it for myself. Is there any way to specify what kind I prefer?

alegr1

1 Feb 2012 11:19 AM

#

In that customer's network, did they have a domain at all? Looks like not. I don't think computers in a domain have that unlimited sharing option.

They should have enabled sharing for "Domain Users" group. I think this can be easily done with a script. The shared folder will have to have the appropriate ACL added (by cacls).

@Maurits[ms]:

Isn't the share ACL applied on top of the NTFS ACL? Means you need to have NTFS permissions to access the file, before the share ACL will give (or deny) you permissions.

Agrona

1 Feb 2012 11:43 AM

#

"OMG pictures!"

This was my response as well. Perhaps recreating the Windows XP dialog boxes using tables turned out to be too time consuming.

[*You're over-thinking it. Those aren't my pictures! -Raymond*]

ErikF
1 Feb 2012 12:26 PM
#

I run my shares wide open and leave the permissions stuff to the filesystem. I've done this with every version of NT because it gets far too confusing having to compute effective permissions from two places!

The only time when I would ever consider using share permissions is for shares that absolutely have to be read-only (for a provisioning server or something like that) or if I had to share a FAT volume for some reason. Fortunately those are very unlikely for me.

Dave
1 Feb 2012 12:56 PM
#

Funny, our machines fill themselves with *** without having public sharing enabled. Must be another cause behind this...

Nick
1 Feb 2012 2:06 PM
#

To be fair, many small companies have a half dozen computers, no domain, no proper server, and they only want things like file sharing to "just work". Physical security provides access restriction, and a firewall/router provides all the network security they need.

Will
1 Feb 2012 3:34 PM
#

@Nick

Physical security and a "firewall/router" is all fine and dandy until it's not.

Like, say, when the boss's kid brings an infected laptop in and uses the wifi for "homework", or someone "accidentally" opens some random porn malware.

Then suddenly all their corporate data is gone, or being sent to the owners of some botnet. Probably along with a copy of their MYOB database or Excel spreadsheet containing your credit card.

Dan
1 Feb 2012 5:28 PM
#

Actually, this isn't *neccesarily* a ridiculous thing to do, depending on the context.

Example: At my office, we occasionally run training. We have a VM on our network that acts as a server for training. The machine is always rolled back to the initial state before a training session.

Training involves people downloading the software in which they are being trained onto their machines, which are temporarily added to our network.

So: Do we want to force everyone on that network to have a login on the training server? Could be done. But it's a bit tedious and redundant, considering they'll only be there for a few days.

So we do an alternative. We set up the VM to disable password-protected sharing.

The shared folders on that VM that we don't want just anyone to access explicitly require a member of the Users group. Trainees cannot access these folders without a password.

However, the shared folders that we *do* want the trainees to access has Users, Guest and ANONYMOUS LOGON.

In all cases, write/modify permissions are restricted to administrators.

This works. Well... And the VM is only up and running during training anyway, so no big deal.

In the right circumstances, this particular scenario isn't all that crazy.

> [*But these people wanted to automate this setting. In other words, they planned to set up hundreds of machines in this configuration, not just a few. -Raymond*]

cheong00
1 Feb 2012 6:15 PM
#

I have two thoughts:

1) The support people who cannot take care of this shall not be allowed to take the job.

2) On the second thought, from the dialog, these machines clearly hadn't join domains. Maybe it's just small company with 4-6 people that cannot afford the money to hire real I.T. people.

Drak
1 Feb 2012 10:28 PM
#

@gm: If your computer has already joined another homegroup it cannot join this homegroup. Also, if the network is not set up as a 'home' network it cannot join the homegroup. Oh, and if your Windows 7 is not at least Home Premium, no homegroup for you!

asdbsd
2 Feb 2012 2:31 AM
#

It might be that their network is well protected from outside and they only use shares for exchanging files (so what if there's some spam in temporary folder, just delete it).

Personally, I always enable guest account access from network because why the hell disable it? It's just as good a part of a security system as any other. If I wish to share something to everyone, guests included, then that's my decision. If I didn't want the whole world to attend the event, I wouldn't have included everyone in the visitors list.

Crescens2k
2 Feb 2012 8:28 AM
#

@asdbsd

Well, it is a good thing that on Windows that the Everyone group doesn't include guests then.

If they need to share files, then doing one simple thing like adding a common user/password pair to all machines would be much more preferable to enabling guest. You see, enabling guest gives everything the chance at an elevation of privileges attack on the system, but using a common username/pass only gives the people who know about the user account. Enabling guest would also allow the possibility of network transmitable malware to propegate easily. So no, I wouldn't class guest a good part of any network security system.

Well, if you like a gaping security hole then it is up to you.

640k
2 Feb 2012 2:37 PM
#

"Then suddenly all their corporate data is gone, or being sent to the owners of some botnet. Probably along with a copy of their MYOB database or Excel spreadsheet containing your credit card."

That's actually usually a calculated risk. To spend a week or two of work on playing windows' impossible "security" game, when you are in a hurry, may cost you a missed deal with a customer.

This is a risk which small startups often take, comparable to security surveillance, which they cannot afford, and they get robbed. Or cannot afford any backup harddisk, and disk crashes.

It's not fatal in most cases, some employee usually has a copy somewhere. Big deal.

I would personally never dream on working at such a company of course, but I know of many.

aylivex
2 Feb 2012 11:28 PM
#

@Drak Windows 7 Home Basic and Starter, as well as domain-joined computers, can't create a new home group but they can join an existing one.

asdbsd
3 Feb 2012 3:35 PM
#

@Crescens2k:

Enabling Guest by itself does nothing. It does not "allow for privilege escalation" and doesn't "help malware propagate".

It only lets you decide what you want. If you don't want to share stuff with everyone, you can continue sharing it only with selected people.

JohnL
6 Feb 2012 9:40 AM
#

"But these people wanted to automate this setting. In other words, they planned to set up hundreds of machines in this configuration, not just a few. -Raymond"

Or they want to set up a few machines again and again. That actually fits with the training lab scenario, since at the end of the course they want to hit a button and have all the machines revert back to a consistent state, ready for the next group of students