

Offer Remote Assistance – "Permission denied" – Windows XP SP2

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-01/1202.html

From: Research Services (*key_at_lamar.n0-sp@m.colostate.edu.NO*)

Date: 01/14/05

Date: Fri, 14 Jan 2005 09:07:06 -0700

We are having problems getting "Offer Remote Assistance" to work in our Child Domain (part of an Active Directory Forest). In Offer Remote Assistance, when we Click the Connect Button from a Windows XP SP2 computer with Windows Firewall Enabled, an error box "Permission denied" is displayed immediately, as if it never even gets far enough to try to communicate to the destination XP SP2 computer (no hard drive activity, no event log activity, no dropped traffic by the firewall). Interestingly, when we put in a W2K3 box as the destination, we received a different error "Access to the requested resource has been disabled by your administrator" and it actually does "talk" to the W2K3 box over the network as you can hear the disk grind at the moment it attempts to connect. We have not used GPOs to Enable Remote Assistance on our W2K3 boxes.

So, the list of what we have done with related Microsoft KB Articles:

<http://support.microsoft.com/?kbid=301527>

- Through Group Policy, have Enabled both 'Solicited Remote Assistance' and 'Offer Remote Assistance' at
Computer Configuration / Administrative Templates / System / Remote Assistance
- Added a couple of Domain Admin Groups who are also in the Local Administrators group on all computers with the <domain>\<group> format to the Group Policy above
- Added/Changed the DCOM Registry Key as such on ALL involved computers:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole]
"EnableDCOM"="Y"
- Opened all of the items below in the Windows Firewall through Group Policy:
% WINDIR%\SYSTEM32\Sessmgr.exe:*.Enabled:Remote Assistance
% WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe:*.Enabled:Offer Remote Assistance
% WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe:*.Enabled:Remote Assistance – Windows Messenger and Voice
135:TCP:*.Enabled:Remote Assistance Port

microsoft.public.windowsxp.security_admin: Offer Remote Assistance – "Permission denied" – Windows XP SP2

– We have even Enabled to "*" 'Allow remote administration exception', 'Allow file and printer sharing exception' and 'Allow Remote Desktop exception' in the Firewall as well

<http://support.microsoft.com/?kbid=884910>

– Even though all of our computers are Windows XP SP2, since we have left this group Policy as 'Not Configured' we don't believe it applies to us. (And attempting to modify this as KB stated caused all sorts of other DCOM related problems)

<http://support.microsoft.com/?kbid=310629>

Simple File Sharing is disabled since all computers are within our Domain (Domain Computers), so this article doesn't apply to us. We have verified that this checkbox is NOT selected on all of the computers involved.

Right-Click, Properties on 'My Computer', Remote Tab on all involved computers has the 'Allow Remote Assistance invitations to be sent from this computer' checked.

Resultant Set of Policies (RSOP) verifies that all appropriate Group Policies are being applied correctly.

All involved computers are on the same subnet and no other firewalls exist other than the Group Policy-enforced Windows Firewall configured as mentioned above. In fact removing the Windows Firewall on both the 'Expert' and 'Novice' computers generates the same error message 'Permission denied'.

The 'Remote Desktop Help Session Manager' service is set to Automatic and in the Running state on the computer that the 'Offer Remote Assistance' is being made from and under the security context of a Local AND Domain Administrator account – this user is part of one of the groups added to the Group Policy above.

'Offer Remote Assistance' is being initiated from a Shortcut to:

hpc://CN=Microsoft%20Corporation,L=Redmond,S=Washington,C=US/Remote%20Assistance/Escalation/unsolicited

Remote Desktop works correctly for all involved computers.

Generating a Remote Assistance request and sending via email works perfectly. Only Unsolicited (Offer) Remote Assistance does not work.

We use Group Policy to "lock down" most of the Security Settings under 'User Rights Assignments' and 'Security Options'. See list of settings below:

USER RIGHTS ASSIGNMENTS

Policy Security Setting

Access this computer from the network MYDOMAIN\Domain Admins,MYDOMAIN\Domain Users

Act as part of the operating system

Add workstations to domain

Adjust memory quotas for a process LOCAL SERVICE,NETWORK SERVICE,Administrators

Allow logon through Terminal Services Administrators,Remote Desktop Users
Back up files and directories Administrators
Bypass traverse checking Users
Change the system time MYDOMAIN\Domain Admins,MYDOMAIN\Domain Users,Administrators
Create a pagefile Administrators
Create a token object
Create global objects Administrators,INTERACTIVE,SERVICE
Create permanent shared objects
Debug programs Administrators
Deny access to this computer from the network
Deny logon as a batch job
Deny logon as a service
Deny logon locally
Deny logon through Terminal Services ASPNET
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system MYDOMAIN\Domain Admins,Administrators
Generate security audits LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication ASPNET,Administrators,SERVICE
Increase scheduling priority Administrators
Load and unload device drivers Administrators
Lock pages in memory
Log on as a batch job
Log on as a service NETWORK SERVICE
Log on locally MYDOMAIN\Domain Admins,MYDOMAIN\Domain Users,Administrators
Manage auditing and security log Administrators
Modify firmware environment values Administrators
Perform volume maintenance tasks Administrators
Profile single process Administrators
Profile system performance Administrators
Remove computer from docking station Administrators,Users
Replace a process level token LOCAL SERVICE,NETWORK SERVICE
Restore files and directories Administrators
Shut down the system Administrators,Users
Synchronize directory service data
Take ownership of files or other objects Administrators

SECURITY OPTIONS

Policy Security Setting
Accounts: Administrator account status Not Applicable
Accounts: Guest account status Not Applicable
Accounts: Limit local account use of blank passwords to console logon only
Enabled
Accounts: Rename administrator account Not defined
Accounts: Rename guest account Not defined
Audit: Audit the access of global system objects Disabled
Audit: Audit the use of Backup and Restore privilege Disabled
Audit: Shut down system immediately if unable to log security audits
Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language
(SDDL) syntax Not defined

DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax Not defined

Devices: Allow undock without having to log on Disabled

Devices: Allowed to format and eject removable media Administrators

Devices: Prevent users from installing printer drivers Disabled

Devices: Restrict CD-ROM access to locally logged-on user only Disabled

Devices: Restrict floppy access to locally logged-on user only Disabled

Devices: Unsigned driver installation behavior Warn but allow installation

Domain controller: Allow server operators to schedule tasks Not defined

Domain controller: LDAP server signing requirements Not defined

Domain controller: Refuse machine account password changes Not defined

Domain member: Digitally encrypt or sign secure channel data (always) Enabled

Domain member: Digitally encrypt secure channel data (when possible) Enabled

Domain member: Digitally sign secure channel data (when possible) Enabled

Domain member: Disable machine account password changes Disabled

Domain member: Maximum machine account password age 7 days

Domain member: Require strong (Windows 2000 or later) session key Enabled

Interactive logon: Do not display last user name Enabled

Interactive logon: Do not require CTRL+ALT+DEL Disabled

Interactive logon: Message text for users attempting to log on

Interactive logon: Message title for users attempting to log on Not defined

Interactive logon: Number of previous logons to cache (in case domain controller is not available) 0 logons

Interactive logon: Prompt user to change password before expiration 14 days

Interactive logon: Require Domain Controller authentication to unlock workstation Enabled

Interactive logon: Require smart card Not defined

Interactive logon: Smart card removal behavior Lock Workstation

Microsoft network client: Digitally sign communications (always) Disabled

Microsoft network client: Digitally sign communications (if server agrees) Enabled

Microsoft network client: Send unencrypted password to third-party SMB servers Disabled

Microsoft network server: Amount of idle time required before suspending session 720 minutes

Microsoft network server: Digitally sign communications (always) Disabled

Microsoft network server: Digitally sign communications (if client agrees) Enabled

Microsoft network server: Disconnect clients when logon hours expire Enabled

Network access: Allow anonymous SID/Name translation Not Applicable

Network access: Do not allow anonymous enumeration of SAM accounts Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares Enabled

Network access: Do not allow storage of credentials or .NET Passports for network authentication Enabled

Network access: Let Everyone permissions apply to anonymous users Disabled

Network access: Named Pipes that can be accessed anonymously

Network access: Remotely accessible registry paths

System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Control\RemoteAssistance\System\RemoteAssistance\Applications,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP

Server,Software\Microsoft\Windows
NT\CurrentVersion,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal
Server,System\CurrentControlSet\Control\Terminal
Server\UserConfig,System\CurrentControlSet\Control\Terminal
Server\DefaultUserConfiguration
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accounts Classic –
local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password
change Enabled
Network security: Force logoff when logon hours expire Enabled
Network security: LAN Manager authentication level Send NTLMv2 response
only\refuse LM & NTLM
Network security: LDAP client signing requirements Require signing
Network security: Minimum session security for NTLM SSP based (including
secure RPC) clients Require message integrity,Require message
confidentiality,Require NTLMv2 session security,Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including
secure RPC) servers Require message integrity,Require message
confidentiality,Require NTLMv2 session security,Require 128-bit encryption
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives and all folders
Disabled
Shutdown: Allow system to be shut down without having to log on Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing,
and signing Disabled
System objects: Default owner for objects created by members of the
Administrators group Object creator
System objects: Require case insensitivity for non-Windows subsystems
Enabled
System objects: Strengthen default permissions of internal system objects
(e.g. Symbolic Links) Enabled

Any suggestions would be greatly appreciated – thank for help in advance.