

HelpServicesGroup

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-02/0143.html>

From: Max Polk (x@x.invalid)

Date: 02/08/03

From: Max Polk <x@x.invalid>
Date: Sat, 08 Feb 2003 22:24:00 GMT

Windows XP home comes with a special local group called "HelpServicesGroup" and a special user in it called "SUPPORT_#####", where each # is a decimal or hex digit.

Also by default requests for Remote Assistance is enabled.

This is described in a few places:

> From <http://www.activewin.com/reviews/previews/windowsxp/admin/misc.shtml>

> *The HelpServicesGroup seems to be a little strange. The only member is a user called "Support_#####" which has a description of "This is a vendor's account for the Help and Support." This user account has the options of "Password Never expires" and "User can not Change Password" enabled. Could this be a back door to your system for Microsoft?*

> From http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/lsm_local_groups.asp :

> *This group allows administrators to set rights common to all support applications. By default, the only group member is the account associated with Microsoft support applications, such as Remote Assistance. Do not add users to this group.*

To get rid of these, first disable remote assistance by going to My Computer | Properties | Remote, then uncheck "Allow Remote Assistance invitations to be sent from this computer."

Then, find out the name of the mystery user added by Microsoft by typing in a command prompt:

```
net localgroup HelpServicesGroup
```

It lists the members of that group, should be just one beginning with "SUPPORT". The comment for the group is "Group for the Help and Support

Center".

If you are curious, to list information about the user type the following replacing the # with the user name you found above:

```
net user SUPPORT_#####
```

The comment for the user is "This is a vendor's account for the Help and Support Service". Delete that user with:

```
net user SUPPORT_##### /delete
```

Then get rid of the HelpServicesGroup group itself with:

```
net localgroup HelpServicesGroup /delete
```

I grant this to the public domain. -- Max Polk (maxpolk@lycos.com)