

Re: Delegating permission to add computers to the domain

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-03/1592.html

From: David Everett [MSFT] (*deverett_at_online.microsoft.com*)

Date: 03/26/04

Date: Fri, 26 Mar 2004 14:39:10 -0600

Hello Jon,

Steps 1– 6 will give the delegated user or group the ability to Add workstations to a specified OU. In the event they ever have to rejoin a workstation to the domain Step 7 will give them the right to re-add a computer account when they were not the ones to join it to the OU the first time. If you do not want them to have the ability to re-Add then stop after Step 6.

1. From the the Active Directory Users and Computers snap-in, click Advanced Features on the View menu so that the Security tab is exposed when you click Properties.

2. Right-click the Computers container, and then click Properties.

3. On the Security tab, click Advanced.

4. Add the group that you want to allow re-adding workstations with the same name.

5. Make sure the "This object and all child objects" option is displayed in the "Apply onto" box.

6. From the Permissions box, click to select the Allow check box next to the "Create Computer Objects" and "Delete Computer Objects" ACEs, and then click OK.

7. For the User to have the rights to re-install a system they did not join to the OU initially they will require "Read all Properties," "Write all Properties," and "Reset and Change Password" rights on the computer object. To do this Edit their existing rights in Advanced Security and click "Apply onto...". In the drop-down box select Computer Objects and then set Allow on the following:

- a. Read all Properties
- b. Write all Properties

microsoft.public.windows.server.active_directory: Re: Delegating permission to add computers to the domain

- c. Change Password
- d. Reset Password

--

David Everett

Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights.

"Jon Paskett" <paskettj@email.NOSPAM.com> wrote in message

news:up#ExIqEEHA.1544@TK2MSFTNGP11.phx.gbl...

> OS = Windows Server 2003

>

> I need to delegate permission to a group of users to add computers to the

> domain in their OU only. Creating a custom task allowing Object Type =

> Computer Objects, Create/Delete objects with Full Control Permission in

the

> custom delegation wizard. However, this does not allow group members to

add

> the computer to the domain. AD says user does not have permission.

>

> TIA

>

> Jon

>

>