

Re: Microsoft Security & Configuration Tool (MSCT)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-05/0379.html>

From: David Dickinson [MVP] (eis.no-spam@softhome.net)

Date: 05/18/02

From: "David Dickinson [MVP]" <eis.no-spam@softhome.net>

Date: Sat, 18 May 2002 01:21:41 -0600

Halomoan Chow wrote:

- > *I used MSCT for securing my server. I imported basicsv.inf and*
- > *secwks.inf as the templates.*
- > *Now after the security configuration, many softwares that I need to*
- > *install into the server become problem.*
- > *Many of them cannot register specific .dll files even I use the*
- > *administrator account.*
- > *My question are :*
- > *1. Why the software cannot register .dll files even logon as the*
- > *administrator account ? Are there any way to register the files ?*
- > *2. How to undo the security configuration that I had already applied*
- > *? So put the server back as before.*

This question is more appropriate for

<news://msnews.microsoft.com/microsoft.public.win2000.security>

However, the answer depends upon how you applied the templates (and we need to know more about your network configuration). For the purposes of this discussion, I'll assume that you assigned the basicsv.inf template to the domain controller and secwks.inf to the domain, and that the server is subject to the restrictions in secwks.inf in Active Directory Users and Computers (i.e., that secwks.inf is the Default Domain Policy and that basicsv.inf is the Domain Controller Security Policy, and they have been applied correctly in AD Users and Computers and AD Sites and Services).

If the domain controller should not be subject to secwks.inf, there are several ways to accomplish the desired effect. For instance, you can create different organizational units (OUs) for the servers and workstations and apply the group policy objects (GPOs) to their respective OUs. Keep in mind the order of precedence of GPO application: sites are first, then domains, then OUs (which have precedence over the others). Also note that you can set a GPO so that it is not overridden by other GPOs. In your case (if I am assuming the correct configuration of your network), in AD Users and Computers, you can right-click Domain Controllers, select Properties, click

microsoft.public.security: Re: Microsoft Security & Configuration Tool (MSCT)

the Group Policy tab, click the Domain Controllers Policy (there would be only one in the scenario you may have given), click the Options button, and put a checkmark next to No Override. That would prevent the domain policy from secwks.inf from influencing the DC.

Assuming, of course, that my assumptions are correct.

To "undo" what you have done, import the setup security.inf template and delete the others. Unfortunately, this will leave you with very little security.

For more information, see

MSDN Group Policy Reference

http://msdn.microsoft.com/library/en-us/gp/rsrc_gp.asp

A List of Windows 2000 White Papers and Technical Resources (Q298447)

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q298447>

Windows 2000 Administration: Security Services

<http://www.microsoft.com/windows2000/techinfo/administration/default.asp#section5>

Windows 2000 Resource Kits Online Books and References

<http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp>

and be prepared to spend some time reading.

--

David Dickinson, MVP (Security)

EveningStar Information Services

Las Cruces, NM USA

Summary of Microsoft Security Bulletins

<http://www.zianet.com/bwd/securitybulletins.asp>