

Re: SUS, IIS Lockdown and Terminal Server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-05/0042.html>

From: Torgeir Bakken (MVP) (*Torgeir.Bakken-spam_at_hydro.com*)

Date: 04/30/03

Date: Wed, 30 Apr 2003 23:10:48 +0200

Rob Smyth – MCSE CCNP CISSP wrote:

- > *As part of the SUS install it runs IIS Lockdown, you are*
- > *not given a chance to modify this – Be warned – DO NOT*
- > *INSTALL SUS on a PRODUCTION WEB SERVER – it will disable*
- > *FTP, Session states and many other things along with*
- > *creating new web users accounts – What fun.*
- >
- > *(snip)*
- > *I was unable to find any Q articles or referances in any*
- > *group.*

Hi

This has been discussed in the SUS newsgroup
(microsoft.public.softwareupdatesvcs) several times, here are some threads:

<http://groups.google.com/groups?th=645ca24d3396f834>

<http://groups.google.com/groups?th=c78d573d5868cd4e>

<http://groups.google.com/groups?th=fd726b0afd156864>

More here:

http://groups.google.com/groups?q=+%22iis+lockdown%22+group:microsoft.public.softwareupdatesvcs.*

URL to the group softwareupdatesvcs for those who uses the not so good Web
interface to access the newsgroups:

<http://communities.microsoft.com/Newsgroups/default.asp?ICP=MSCOM&sLCID=US&newsgroup=microsoft.public>

Microsoft references about this issue:

Server Requirements and Recommendations for Installing Microsoft Software
Update Services

<http://support.microsoft.com/?kbid=322365>

<quote>

Existing Server Recommendations

If you are going to install SUS on an existing server, the administrator must

follow these steps
(snip)

4. If IIS is not installed, physically disconnect the server from the network before you install IIS. After you install IIS, install any IIS security patches, and then run the IIS Lockdown tool before you connecting the server to the network again.

</quote>

<http://www.microsoft.com/windows2000/windowsupdate/sus/sp1relnotes.asp>

<quote>

Better integration with IIS lockdown tool

</quote>

SUS_sp1_install.doc (SP1 Release notes document):

<quote>

Installing IIS Lockdown

If you are running IIS on a computer running Windows 2000 Server, install the latest versions of IIS Lockdown tool and the URL Scanner from

<http://microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp>.

Microsoft strongly recommends that you install these tools to help keep your IIS servers secure. The IIS Lockdown Wizard works by turning off features of IIS, thereby reducing the security risk exposure.

Note:

If neither IIS Lockdown nor URL Scanner is installed on the Windows 2000 Server where you install SUS 1.0, SUS 1.0 SP1 setup will install and configure IIS Lockdown version 2.0 and URL Scanner version 2.5 for you. If one of these tools is already installed, the setup program will not install either of them. SUS setup will not change settings for either of these tools, and it will preserve your backup of the IIS metabase.

(snip)

Better integration with IIS Lockdown

If either IIS Lockdown or URL Scanner has been installed on the server, SUS server setup will not install either of them. It will not change settings for either of these tools. SUS setup will preserve your backup of the IIS metabase.

</quote>

"Deploying Microsoft Software Update Services" white paper (SUS_Deployguide_sp1.doc) contains 4 pages about this.

<quote>

Appendix A: Understanding Security and Software Update Services Setup 66

(snip)

IIS Lockdown Configuration page 67

What happens to IIS Lockdown when I uninstall Software Update Services? page 68

</quote>

<http://www.microsoft.com/technet/security/tools/tools/sadsus1.asp>

<quote>

During installation, SUS runs the IIS Lockdown Tool to secure IIS on the SUS server. This lockdown prevents an intruder who has cracked into your SUS server from accessing AU clients. The IIS Lockdown Tool disables options that present security risks, so it might break existing Web applications. If your SUS server hosts other Web applications and those applications depend on components such as WWW Distributed Authoring and Versioning (WebDAV), Microsoft FrontPage Server Extensions, or FTP, you might run into problems. Although you can get SUS to coexist with these applications, you might need to reenable certain options after installing SUS. For a full description of the changes SUS makes to IIS, see Appendix A in the "Deploying Microsoft Software Update Services" white paper.

</quote>

--

torgeir

Microsoft MVP Scripting and WMI, Porsgrunn Norway

Administration scripting examples and an ONLINE version of the 1328 page Scripting Guide: <http://www.microsoft.com/technet/scriptcenter>