Feature

Protect Your Web Server with the IIS Lockdown Tool

to top

Last week we talked about the URLScan tool. In case you missed it, the URLScan tool is an ISAPI filter that you can install on an IIS 5.0 computer. This filter examines the HTTP header information and compares it to settings you create in the URLScan.ini file. If the request doesn't meet the requirements set forth in the configuration file, it is dropped. The trick is figuring out how to configure the URLScan.ini file to work with the roles you've set forth for your Web server.

This is where the IIS Lockdown tool becomes your best friend. The Internet Information Services (IIS) Lockdown Tool allows you to automate many different security configuration settings that affect IIS services. Best of all, the URLScan tool is integrated with the IIS Lockdown tool. This integration allows you to use a simple point and click interface to configure URLScan.ini file settings. You don't have to muck around with the error-prone process of manually configuring text files.

The IIS Lockdown Wizard performs many different functions. Some of these include:

- Security configuration based on templates for common Web server roles. Some of these server roles include: FrontPage Web Server, Outlook Web Access Server and SharePoint Team Server.
- Integration of the URLScan tool with the IIS Lockdown Tool. The settings in the Urlscan.ini file are customized to match the settings of the server role template you select.
- Ability to disable or remove IIS services that are not required based on the template settings, such as removing the NNTP service when it's not used on a FrontPage Web server.

The IIS Lockdown tool is a real boon to IIS administrators in that it automates most of the unpleasant tasks involved with securing the Web server. One of the things I like most about it is that if the security configuration whacks some aspect of your server's functionality, you can easily undo the changes you made. You're not stuck wondering what the heck the tool did, and then trying to figure out how to fix what it broke.

Let's go through the procedures you use to secure the server using the IIS Lockdown tool, and then how to undo the changes after you've made them.

Install and Run the IIS Lockdown Tool

Perform the following steps to install and use the IIS Lockdown Tool:

1. Download the IIS Lockdown tool here.
2. Double click on the iislockd.exe file.
3. On the first page of the Internet Service Lockdown Wizard, read the explanatory text. Note that you can undo any changes made by the Wizard. Click Next.

4. On the license agreement page, read the END-USER LICENSE AGREEMENT and click the I Agree option button. Click Next.
5. On the Select Server Template page, read the list of available Server templates. In this example, select FrontPage Server Extensions. Place a checkmark in the View template settings checkbox. Click Next.
6. On the Internet Services page, note that Web service (HTTP) is already selected. The reason for this is that Web service is the only service required by FrontPage Web sites. The other IIS services are not selected. If you do not select any of the other services, then they will be disabled. If you enable the Remove unselected services option, the services will be removed from the server. In this example, select the E-mail service (SMTP) and click Next.
7. On the Script Maps page you can select which script maps to disable on the Web server. Note that Active Server Pages (.asp) is not selected because this option is required to run FrontPage Web sites. Accept the default settings and click Next.
8. On the Additional Security page, you can select which virtual directories should be removed from the Web server. You also have the option to set permissions on files. The last option on the page allows you to disabled Web Distributed Authoring and Versioning (WebDAV). If this option is disabled, users will not be able to create Web Folders to access the Web server. Accept the default settings and click Next.
9. On the URLScan page you can choose to install the URLScan utility. This utility installs itself as an ISAPI filter and will screen inbound HTTP requests based on rules you configure in the urlscan.ini file. In this example we will install the URLscan tool. Click Next.
10. On the Ready to Apply Settings page, review the changes that will be made to the server. If these changes are acceptable to you, click the Next button. If you want to change any of the settings, you can click the Back button and make the appropriate change. Click Next.
11. On the Applying Security Settings page, you can see the changes being made to the server security configuration. When the changes are complete, you will see Finished in the Status box. After the changes are made, click on the View Report button to view the changes that were made to the server. Note on the last line of the report that the changes are written to a log file name oblt-log.log that can be used to reverse the changes. Close Notepad to close the report.
12. Click Next on the Applying Security Settings page.
13. Click Finish on the Completing the Internet Information Services Lockdown Wizard page.

Test the server's functionality after you've made the changes. Make sure you test every aspect you can think of before bringing the server back into production. I highly recommend that you use VMware to mirror your server environment and test the configuration using the VMware virtual machine. If the configuration passes muster, then you can implement the same configuration on the live server.

Undoing the IIS Lockdown Tool Changes

If for some reason the server does not perform as expected, you can undo the changes made by the Wizard. Note that the Wizard can undo

only the changes by the Wizard. If you made manual changes to the server configuration, the Wizard will not be able to undo those changes.

To undo the changes made by the Wizard, perform the following steps:

1. Double click the iislockd.exe file.
2. On the This Server Was Already Configured page, read the explanatory text. Click Next.
3. An Internet Information Services Lockdown Wizard will appear to inform you that the process will undo the changes made when you last ran the Wizard. Click Yes to continue.
4. On the Restoring Security Settings page you can see the previous settings restored. When the process is complete you will see Finish in the Status area. Click Next.
5. Click Finish on the Restoration Complete page.

Summary

The IIS Lockdown Tool allows you to configure security for an IIS 5.0 Web server using a simple, but powerful, graphic interface. This tool integrates with the URLScan ISAPI filter and automatically configures the filter settings to match the server role you have chosen for the server. I highly recommend that you download and test the IIS Lockdown tool and use it on your publicly (and perhaps privately) accessible Web servers.

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

Q and A's

to top

Question:

Mr. Bill,
Riddle me this: I like to have desktop shortcuts. I'm running Office 2000 with Windows 2000 Pro for an OS. I want to put shortcuts to Outlook public folders on my desktop. With NT and Win 98, all I have to do is drag the public folder and drop it on the desktop. When I do that with my current machine, I get a popup that asks me if I want to "add an Active Desktop Item to my Desktop?" If I click "Yes" I get another popup, telling me that "Internet Explorer does not support synchronizing with this type of URL."

Here are some other symptoms: I have two Outlook shortcuts on my desktop from when I was running Win 98 that work fine; and it doesn't matter if I have Active Directory running or not--I get the same results--"Internet Explorer does not support synchronizing with this type of URL." I'm running IE 5, v 5.00.2920.000C.

--Semper Fidelis,
--Steve Yousten,
Lieutenant, USMC
Switching Plt OIC, Co B
9th Communications Bn