IIS LockDown 과 URLscan

목차

개요

IIS LockDown은 Windows NT/2000 기반의 서비스들에 대한 보안을 제공해 주는 통합 도구입니다. IIS LockDown은 IIS의 취약점을 패치해주는 종합선물세트라고 보시면 됩니다. IIS LockDown 을 실행하기 전에 먼저 최신 보안 패치를 모두 적용해야 합니다. 그렇지 않다면 제대로 방어가 되지 않습니다. Windowsupdate.microsoft.com 에서 Critical Update를 수행하여 모든 패치 및 핫픽스를 적용해야 합니다.

실행환경

- OS : Windows NT 4.x 또는 Windows 2000
- IIS : IIS 4.0 또는 IIS 5.0

★ Whistler Server 인 .NET Enterprise/Standard Server에는 IIS LockDown이 포함되어 있습니다. 참고로, .NET Server의 IIS 버전은 5.1 입니다.

특징들

- Server Roles : IIS에 관련된 템플릿을 제공합니다. (Exchange 5.5/2000, Commerse Server, BizTalk, SMS 4.5/2000, SharePoint Portal/Team Server, FrontPage Server Extensions)

- URLscan : 특정한 서버 구성 및 애플리케이션을 설계할 때 관리자가 URLscan을 이용하여 추가적인 보안 정책을 적용할 수 있는 마법사를 제공합니다.
- HTTP, FTP, SMTP, NNTP와 같은 IIS 서비스를 중단 또는 제거할 수 있습니다.
- 응답파일을 지원하여 무인 설치나 스크립트로 지원할 수 있습니다.

프로그램 다운로드

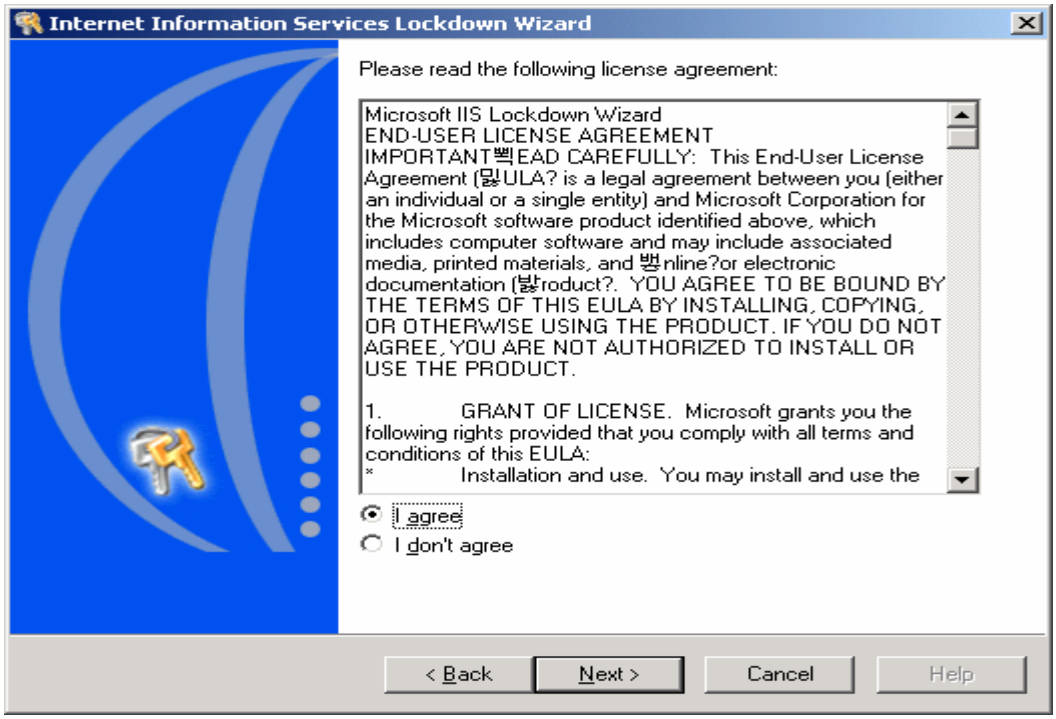
설명 : http://www.microsoft.com/technet/treeview/default.asp?url= /technet/security/tools/locktool.asp

다운로드 : http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961

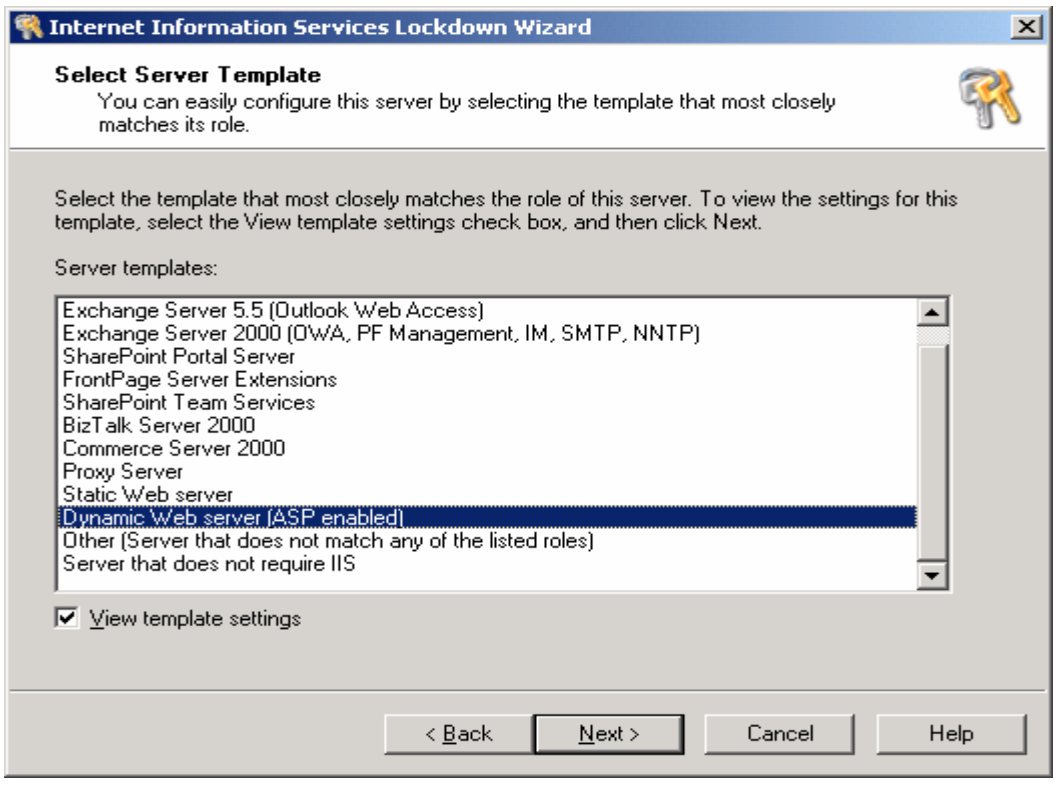
설치방법

1. Windows 2000 인 경우에는 IIS LockDown을 설치하기 전에 Service Pack 2 및 각종 패치 및 핫픽스들을 업데이트한다.
2. 현재 사용중인 IIS 관련 서비스 즉 IIS, FTP, SMTP 등 중에서 사용하는 것이 무엇인지 ASP가 사용중인지를 먼저 확인해야 한다. 이 프로그램의 설치시에 이 서비스들을 중단 또는 제거할 수 있기 때문이다.
3. 다운로드받은 IIS LockDown을 실행하면 아래와 같은 대화상자가 나타나는데 Next 를 클릭한다.

4. 최종사용자 승인(EURA)를 물어본다. 이 프로그램을 사용하려면 당연히 I Agree 를 클릭하고 Next 를 클릭해야 한다.

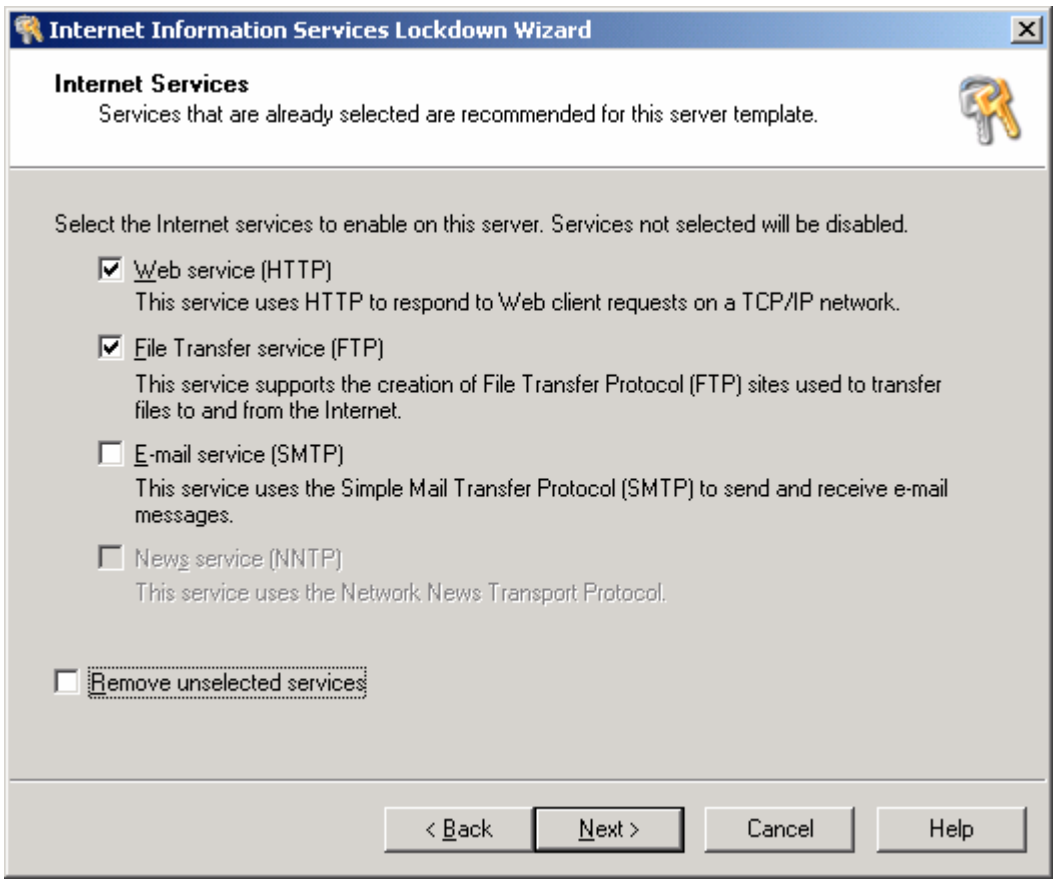


5. 이 화면에서는 IIS에 관련되어 있는 다양한 소프트웨어의 템플릿을 보여준다. 화면 하단에 View Template Setting 을 체크해 두는 것이 낫다. 여기서는 Dynamic Web Server(ASP를 실행하는 웹서버를 말함)에 대해 구성해본다. Dynamic Web Server 를 클릭하고, View Template setting를 체크하고 Next 를 클릭한다.

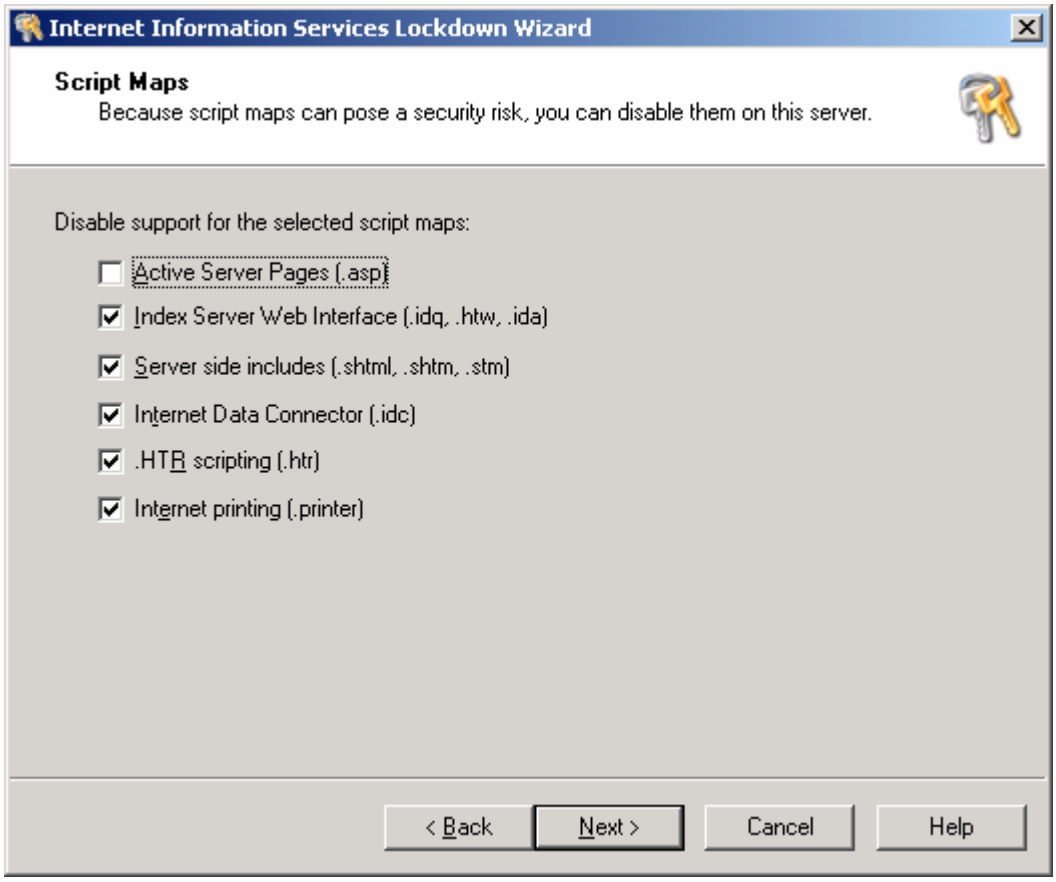


6. 아래와 같이 Internet Services 대화상자가 나타난다. 현재 웹서버에서 어떤 서비스를 운영할지를 미

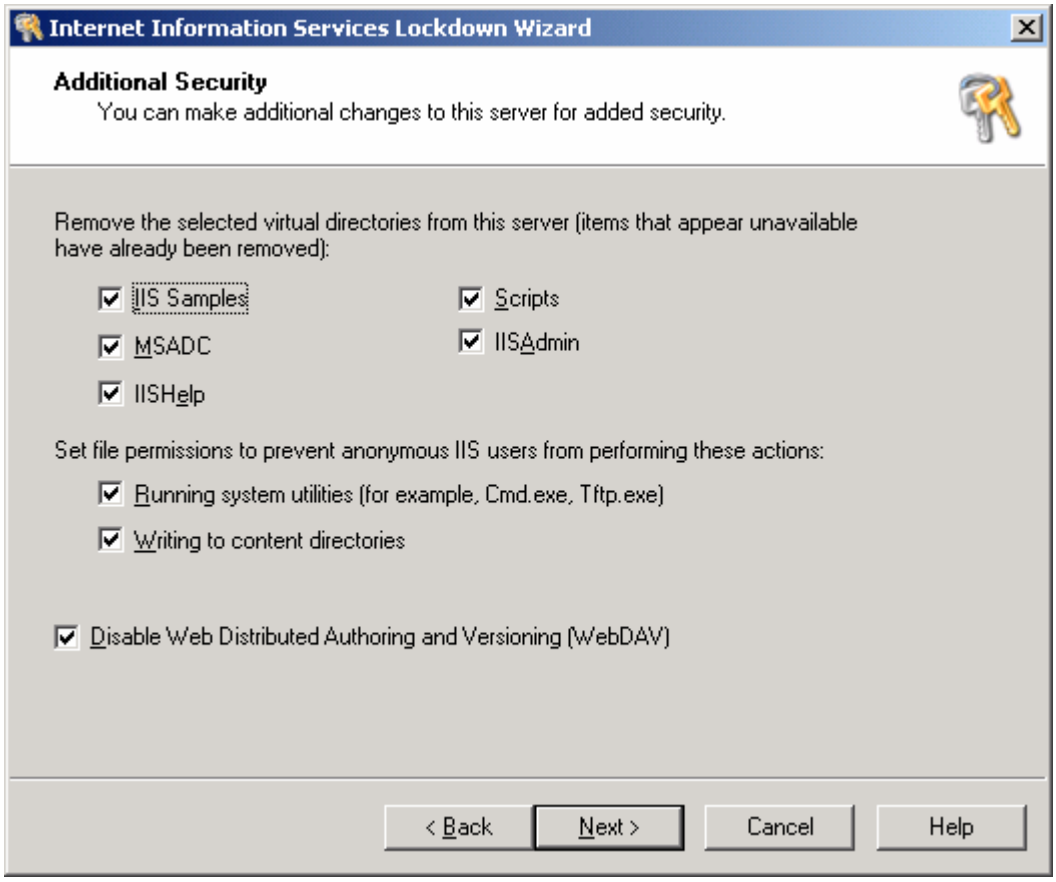
리 파악하여 그 부분만 체크해준다. 만약 사용하지 않는 서비스를 제거하고 싶다면 아래 Remove Unselected Servce 를 체크하면 사용하지 않는 서비스들을 제거된다. 제거한 서비스는 나중에 프로그램 추가/제거 에서 다시 설치할 수 있다. 여기에서는 HTTP와 FTP를 선택하였다.



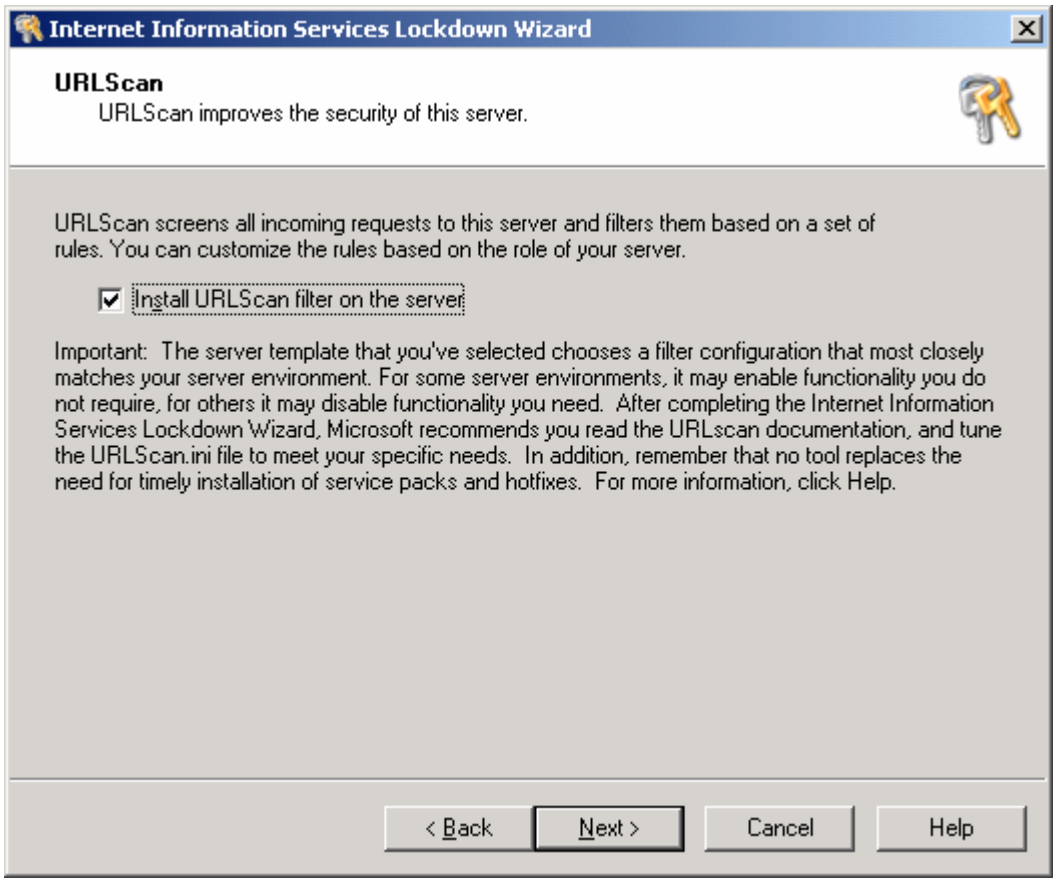
7. 스크립트 매핑에 대한 화면이 나타난다. IIS의 보안에 대한 글을 여러 개 읽다보면 다양한 스크립트 매핑을 제거해야 한다는 것을 알 수 있습니다. 일반적으로 ASP를 구성하는 IIS이므로 첫번째 항목인 ASP만 체크하지 않고 나머지 모두 체크합니다. 매핑에 대한 자세한 내용은 Script Maps 부분을 참고하시기 바랍니다.



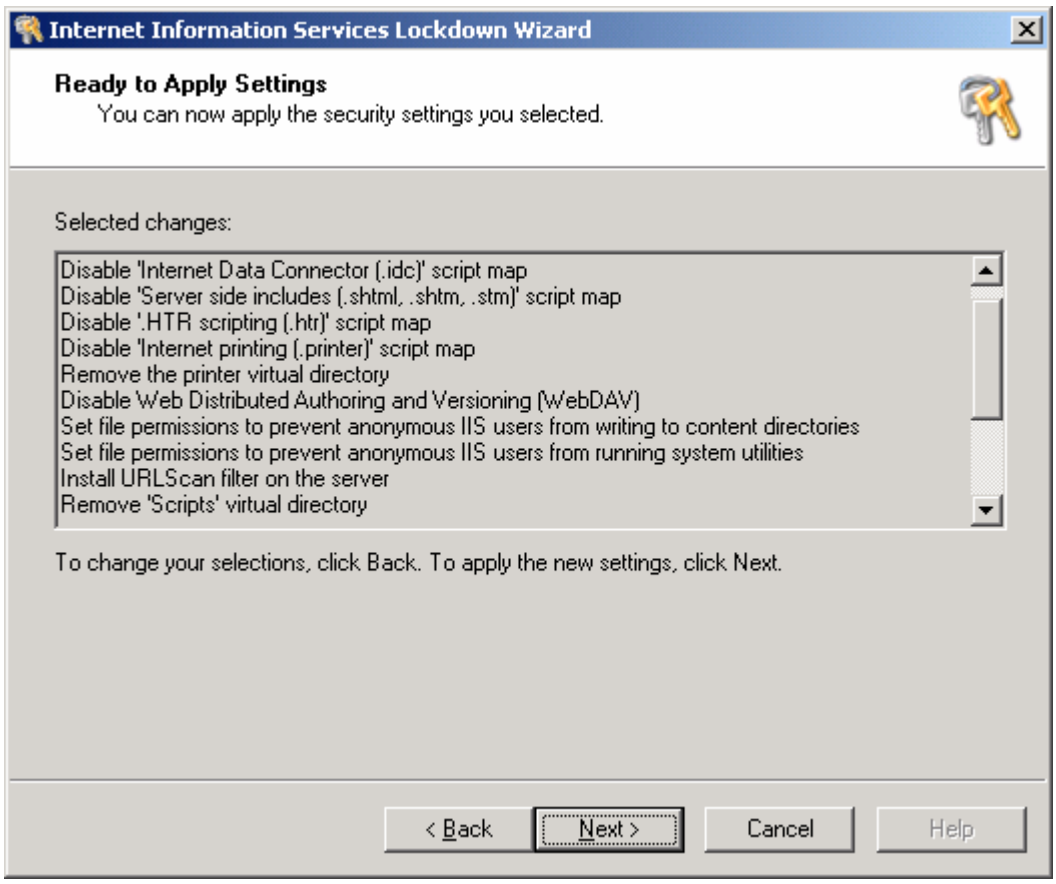
8. 아래와 같이, Additional Security 대화상자가 나타납니다. 일반적으로 InetPub 폴더 아래에는 웹서버를 관리할 수 있게 해주는 여러가지 가상 디렉터리들이 존재합니다. 가장 대표적인 것이 IIS 관리 도구인 IISAdmin 이 있습니다. 하지만, 이러한 부분들은 보안상취약점을 유발할 수 있기 때문에 제거하는 것이 좋습니다. http://www.ntfaq.co.kr/security/view.asp?pid=19 참고.



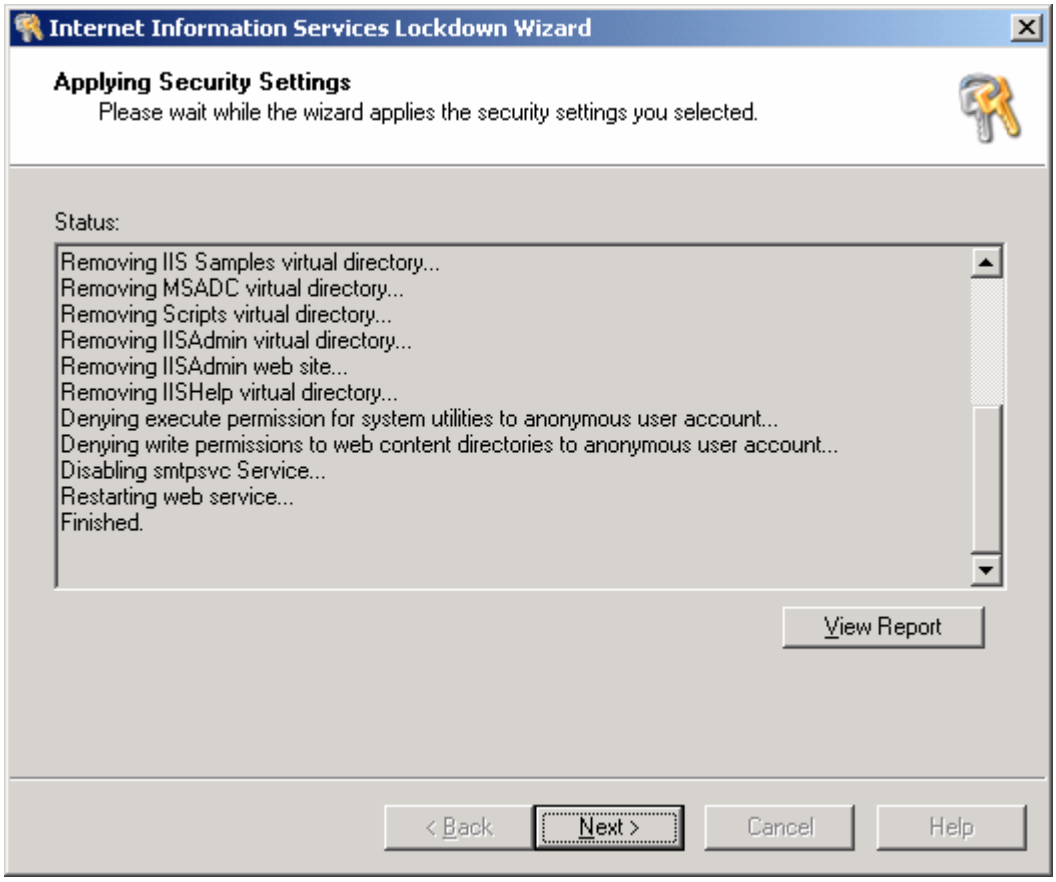
9. 아래와 같이, URLScan을 설치할 지를 묻는 대화상자가 나타납니다. 당연히 설치하는 것이 좋습니다.



10. 현재까지 구성한 설정들을 모두 보여줍니다. 이상없이 설정하였다면 Next 를 클릭합니다. 잘못된 것이 있다면 Back 이나 Cancel을 눌러 적절하게 구성해주면 됩니다.

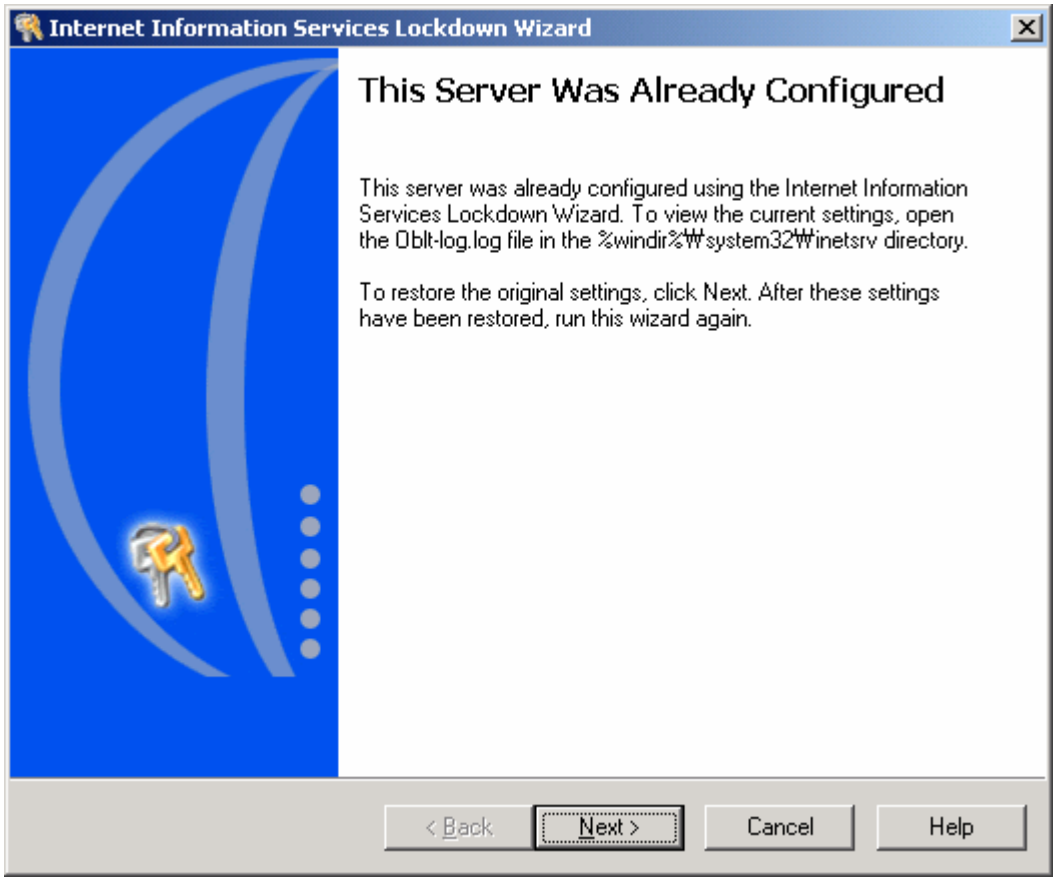


10. 이제 모든 사항이 적용되는 화면이 나타납니다. View report 를 체크하면 현재 서버에 구성한 사항들이 텍스트 파일로 보여줍니다. 이 파일은 보관하여 두는 것이 좋습니다. 로그 파일이 하나 생성되는데 이는 나중에 구성한 내용을 되돌릴 때 사용됩니다. 로그파일의 위치는 %windir%/system32/inetsrv/Oblt-log.log 입니다. Next 를 클릭하면 종료 대화상자가 나타납니다.



상태 되돌리기

여러분이 IIS LockDown을 구성한 이후에는 반드시 여러가지 사항들을 점검해야 합니다. IIS, SMTP 등 사용한다고 구성한 서비스들이 제대로 동작하는지, ASP가 제대로 동작하는지, 기타 필요없는 파일들이 남아 있는지, 인터넷 상에서 웹사이트를 액세스할 수 있는지 모두 확인해야 합니다. 만약 문제가 발생한다면 이전의 상태로 되돌릴 수 있습니다. 이전으로 되돌리려면 IIS LockDown 을 다시 실행하면 됩니다. 실행하면 다음과 같은 화면이 나타납니다. 여기서 Next 를 클릭하면 원래의 상태로 되돌아 갑니다. 하지만 여러 번의 되돌리기를 지원하지 않고 바로 직전에 구성한 상태로 되돌려 지기 때문에 특히 주의해야 합니다.



URLscan 만 설치하기

URLscan을 단독으로 설치하려면 약간 복잡합니다.

1. IIS LockDown 을 실행하고 몇가지 구성을 그냥 Next 를 눌러 넘어갑니다. 그러한 후에 URLscan 설치화면에서 설치를 합니다.
2. IIS LockDown을 다시 실행하여 구성한 사항을 이전 상태로 되돌리기 합니다.
3. URLscan은 제거되지 않기 때문에 이 프로그램 설치되어 있는지 알고 싶을 때 그리고 제거할 때에는 프로그램 추가/제거 를 이용해야 합니다.

Script Maps에 대한 추가정보

IIS에서는 웹서버에 추가되어 새로운 기능을 사용할 수 있게 해주는 ISAPI라는 기술을 제공합니다. IIS의 몇몇 고급 기능은 ISAPI를 사용하여 구현되어 있으며 이를 script maps이라고 하며, 이들 script maps를 제거하여 기능들을 중단시킬 수 있습니다. 다시 한번 말씀드리지만, 이들을 구성하기 전에 먼저 최신의 서비스팩, 업데이트, 패치, 핫픽스를 모두 적용한 이후에 구성해야 합니다. 안그러면 보안상 취약점이 그대로 남아 있을 수 있습니다.

- Active Server Pages(ASP) : ASP는 동적 웹서버를 구축할 수 있게 해주는 기술입니다. ASP 파일은 사용자가 요청을 할 때 서버에서 실행되어 그 결과로 출력된 HTML 문서를 사용자에게 되돌려주는 역할을 해줍니다. ASP를 사용하는 웹서버나 ASP를 필요로 하는 서비스나 OWA(Outlook Web Access)를 사용한다면 반드시 ASP 매핑을 해주어야 합니다. 만약 서버에 정적 HTML(.htm, .html) 등으로만 웹사이트를 만든다면 ASP가 필요없습니다.
- Index Server Web Interface(.IDQ) : dl 기능은 사용자가 Index Server의 웹기반의 쿼리를 생성할 수 있게 해줄 뿐만 아니라 원격에서 관리자가 웹을 통해 Index Server를 관리할 수 있게 해줍니다. IIS LockDown은 이에 관련된 모든 DLL의 ACE를 거부하기 때문에 나중에 나중에 매핑을 되돌리더라도 DLL이 제대로 동작하지 않게 된다. 하지만 표준으로 웹서버를 구성할 수는 있지만 사용자 정의로 Index Server를 사용하여 웹기반으로 검색기능을 처리하지는 못한다. 관리자가 원격에서 index server를 관리하지 않는다면 이 기능은 사용하지 않도록 하는 것이 좋다.
- Server-Side Includes(.SHTML, .SHTM, .STM) : 이 기능은 사용자에게 웹페이지를 전송하기 전에 문자, 그래픽, 애플리케이션 정보들을 추가할 수 있게 해준다. 만약, SSI를 사용한다면 SSI 스크립트를 ASP로 변환하여 사용하는 것이 좋다.
- Internet Data Connector(.IDC) : IDC는 HTML 문서내에 데이터베이스 쿼리를 출력해주는 기술이다. ASP는 IDC를 대체하기 때문에 IDC 스크립트를 ASP로 변환하여 사용하는 것이 좋다. 변환 도구는 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnproasp/html/convertingfromidctoaspidc2asp.asp 를 참고한다.
- HTR Scripting(.HTR) : HTR은 ASP와 비슷한 스크립트로 웹서버를 통해 로그온 암호를 바꾸는 등의 몇가지 스크립트가 유용하게 사용되고 있다. OWA와 암호 변경이 필요하지 않다면 이 기능은 사용하지 않는 것이 좋고, 스크립트는 ASP로 변환해 쓰는 것이 좋다.
- Internet Printing(.printer) : 이 기능은 인터넷을 통해 여러분의 네트워크에 있는 프린트 작업을 관리하거나 전송할 수있게 해준다. IIS LockDown 유틸리티는 이 기능을 영원히 사용할 수 없는 로컬 정책을 생성한다.

응답파일

Windows 2000 설치에는 여러가지 방법이 있는데, 그중 무인(Unattended installation)이라는 것이 있다. 설치에 필요한 모든 사항들을 응답파일이라는 텍스트 파일에 저장하여 이를 이용하는 것인데, IIS LockDown에서도 이 응답파일을 지원한다. 이 것이 있다면, 최적화된 구성을 저장하여 두어 나중에 사용하거나 다른 사람에게 배포하기도 훨씬 간단하게 된다.

간단한 응답파일을 보면서 설명하는 것이 이해가 빠를 거 같군요.

```
[Info]
ServerTypesNT4=sbs4.5, exchange5.5, frontpage, proxy, staticweb, dynamicweb , other,
iis_uninstalled
ServerTypes=MyCustomServerTemplate, sbs2000, exchange5.5, exchange2k, sharepoint_portal,
frontpage, biztalk, commerce, proxy, staticweb, dynamicweb, other, iis_uninstalled
UnattendedServerType=MyCustomServerTemplate
Unattended=TRUE
Undo=FALSE

[MyCustomServerTemplate]
label="My Custom Server Template"

Enable_iis_http=TRUE
Enable_iis_ftp= TRUE
Enable_iis_smtp= FALSE
Enable_iis_nntp= FALSE
Enable_asp= TRUE
Enable_index_server_web_interface= FALSE
Enable_server_side_includes= FALSE
Enable_internet_data_connector= FALSE
Enable_internet_printing= FALSE
Enable_HTR_scripting= FALSE
Enable_webDAV= FALSE
Disable_Anonymous_user_system_utility_execute_rights= TRUE
Disable_Anonymous_user_content_directory_write_rights= TRUE
Remove_iissamples_virtual_directory=TRUE
Remove_scripts_directory=TRUE
Remove_MSADC_virtual_directory=TRUE
Remove_iisadmin_virtual_directory=TRUE
Remove_iishelp_virtual_directory=TRUE
UrlScan_Install=DISABLED
UrlScan_IniFileLocation=
AdvancedSetup =
UninstallServices=TRUE
```

1. iislockd.ini 라는 이름을 가진 텍스트 파일을 만들기 위해 메모장등의 텍스트 편집기를 연다.
2. UnattendedServerType에 원하는 서버 템플릿을 입력한다. 만약 dynamicweb 템플릿을 사용한다면 다음과 같이 하면 된다.

   UnattendedServerType=dynamicweb

3. Unattended 값을 TRUE로 변경한다. 만약, 나중에 상태를 되돌리려면 Undo도 TRUE로 설정해야 한다.
   Unattended=TRUE
   Undo=TRUE
4. [DynamicWeb] 부분에서 원하는 구성을 모두 구성한다.
5. 파일을 저장하고 나온다.

URLscan 설정하기

URLscan은 정확한 URL 이 아닌 %%cc 그외 cmd.exe 등과 같은 형식으로 URL 에 입력시 발생 했던 유니코드 버그에 대한 문제점들을 해결해 준다. 정확한 URL 을 입력 하지 않을 경우는 404 에러가 발생 한다.

1. URLscan의 설치 : URLScan은 IIS LockDown 설치시에 설치할 수 있다. 나중에 삭제할 때에는 프로그램 추가/제거 에서 할 수 있다. URLscan이 어디에 있는지 경로를 알아둔다. 보통 %windir%/system32/inetsrv/urlscan에 위치한다.
2. 웹서버에 추가하기 : Internet Servce manager에서 사용하는 웹사이트의 등록정보를 연다. 여기서 URLscan을 등록한다. 관련된 로그는 urlscan.log에 저장된다.
3. URLScan의 정보를 변경하려면 URLscan이 위치한 폴더내의 urlscan.ini 파일을 수정한다.
4. 웹서버를 재시작한다.

각각의 설정에 대한 자세한 정보는 http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;q307608 를 참고한다. Urlscan.ini 파일을 변경하였을 때에는 반드시 웹서비스를 중지했다가 다시 시작해야 한다. 안 그러면 변경한 내용이 적용되지 않는다.

작성일 : 2001년 12월 12일
작성자 : 문일준(security@ntfaq.co.kr)