White Paper

Cisco BBSM Server Hardening

Overview

Cisco Building Broadband Service Manager (BBSM) is a highly automated service creation platform that enables simple plug-and-play, end-user self-provisioning of services, customizable portal and advertising platforms, web-based management, reporting, and configuration. The Cisco BBSM platform enables property owners and service providers to create tiered service levels to deliver targeted customer offerings. The server-based software supports multiple automated authentication and billing options including credit card, RADIUS, property management system (PMS), and access code.

The Cisco BBSM has been designed for compatibility with Cisco access-layer LAN products to provide a complete solution that enables service providers or property owners to create, market, and operate broadband access services including Long-Reach Ethernet (LRE), 10/100/1000 Ethernet, wireless LAN, and cable. BBSM software is designed to operate with the Windows 2000 Server operating system.

Target Audience

System Engineers, System Administrators, and Network Engineers versed in Windows 2000 Server and BBSM software.

Introduction

The purpose of this white paper is to provide an instructional checklist for hardening a BBSM server. Ideally, the goal of a *hardened* server is to leave it exposed on the Internet without any other form of protection. This paper will describe the hardening of a BBSM appliance, which requires some services and processes exposed to function properly. Think of it as *BBSM Best Practices*. Hardening of BBSM will involve disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files, services, and end points.

Note: It is important to remember that a server should only be *locked down* when all functional and end-to-end tests have already been completed, and the system is ready for customer use. A locked down system, by definition, is one that will not be altered in any way.

Historical Overview

The Internet now provides even the unskilled Internet user the opportunity to download tools that automatically scan the globe for open ports and exploits all operating systems, web servers, databases, etc. By nature, the BBSM server has a multitude of extraneous services and ports that can be locked down and disabled to provide a more secure computing environment.

Business Needs

This instructional paper provides an opportunity for customers to incorporate the BBSM overlay network into their own Best Practices methodology.

Terms and Definitions

The following table provides a list of important terms and definitions.

Terms and Definitions

BBSD	Building Broadband Service Director
BBSM	Building Broadband Service Manager
DoS	Denial of Service
FTP Service - BBSD	BBSD requires an FTP login on port 50500 and uses the BBSD login/user that is created during the BBSM installation.
FTP Service - WEBpatch	WEBpatch is the mechanism in BBSM to remotely upgrade the server software. WEBpatch requires both the FTP service and Anonymous FTP access enabled. Due to the number of FTP based exploits, this paper recommends disabling the FTP service on the BBSM server. To run a patch, a System Administrator must enable the service, run WEBpatch, reboot, and then disable the service. WEBpatch creates a temporary virtual directory under the anonymous account. This occurs so that passwords do not have to be sent over the Internet.
Remote Registry Service	Routing and Remote Access Services (RRAS) depends on this service, and it cannot be disabled.
RPC Service	Internet Information Server (IIS) and many other system critical components require RPC and it cannot be disabled.
Scanning and Auditing Tools	What should I see? A port scanning utility run from the internal (client) network will respond to every port, service, Trojan, and executable query. This is because the ATNAT driver in BBSM is designed to respond to all queries from that network. This not only will confuse hackers, but is essentially an internal protection against those types of investigative attempts. However, it only responds for the internal NIC. The external NIC will report the correct port information. So any scanning/audit tools should be pointed at the external network interface. Remember that different port scanners have different levels of reliability, dated response information, heuristics, and timers. This will affect the types of information returned against a BBSM appliance. A hardened BBSM server should enumerate TCP Ports 25 (SMTP), 110 (POP), 135 (DCE), 443 (SSL), 1433 (SQL). A hardened BBSM server should enumerate UDP Ports 53 (DNS), 68 (BOOTPC), 137 (NetBIOS), 161 (SNMP), 1434 (SQL). Note that even though 135, 137, 161 are enumerated; they are disabled and do not transmit on those ports.
Server Service	The Microsoft Message Queuing Service (MSMQ) depends on this service, and it cannot be disabled.

Hardening the Installation Server - Checklist

1. Configure the IP addresses on your server through the Address Change Wizard and reboot when prompted.
   - Configure and/or verify WEBconfig and switch settings.
   - Verify IP and client connectivity.
2. Install all latest updates from CCO for BBSM WEBpatch. (This requires external Internet connectivity.)
   - Automatic reboots will occur.

3. Disable unnecessary services:
   - Alerter (already disabled)
   - athdmn (Enable if this is a PMS-billable site.) This service does not exist in BBSM Hotspot.
   - Clipbook
   - Computer Browser
   - DHCP Client
   - Distributed File System
   - Distributed Link Tracking Client
   - Distributed Link Tracking Server
   - Fax Service
   - File Replication
   - FTP Publishing Service (This service needs to be enabled when using WEBpatch and then disabled again on reboot.)
   - Indexing Service
   - Internet Connection Sharing
   - Intersite Messaging (already disabled)
   - Kerberos Key Distribution Center (already disabled)
   - License Logging Service
   - Messenger (already disabled)
   - Microsoft Firewall (already disabled)
   - Microsoft H.323 Gatekeeper (already disabled)
   - Microsoft Scheduled Cache Content Download (already disabled)
   - Netmeeting Remote Desktop Sharing
   - Network DDE
   - Network DDE DSDM
   - PMS Test Service (Enable if this is a PMS Billable site.) This service does not exist on the BBSM Hotspot appliance.
   - Print Spooler (Enable if guest web print or print billing is required.)
   - QoS RSVP
   - Removable Storage
   - Smart Card
   - Smart Card Helper
   - Telnet
   - Terminal Services (Enable for remote access, if desired.) This service is enabled on Hotspot by default.
   - TFTP (Enable when required for switch firmware upgrades.) Required for Cable Modem installations.
   - Uninterruptible Power Supply (Enable if you are monitoring a UPS from the BBSM.)
   - WEBprint (enable if required) Service does not exist on the BBSM Hotspot appliance. Requires Print Spooler Service.
   - Windows Time
4. Rename Administrator account and set an appropriate password. Use this procedure:

Step 1. Choose **Start > Programs > Administrative Tools > Computer Management**.

Step 2. Click **Local Users and Groups**.

Step 3. Right-click on the Administrator account to change the name and set the password.

5. Set the sa password. (This applies to BBSM 5.2 and Hotspot.) Use this procedure:

Step 1. From the BBSM Dashboard, go to WEBconfig, and click the **Security/SSL** link in the left pane.

Step 2. Click **Change**.

Step 3. Enter the current password.

Step 4. Enter the new password.

Step 5. Confirm the new password.

Step 6. Click **Submit**.

6. Set the sa Password. (This applies to BBSM 5.0 and 5.1.) Use this procedure:

Step 1. Open the command prompt by choosing **Start > Run**.

Step 2. From the Run window, type **cmd** and press **Enter**.

Step 3. From the prompt, type **`osql -U sa -P "your current password" -Q "sp_password NULL,your new password,sa"`**

Note: Make sure that you enclose your *current password* and your *new password* within double quotation marks.

7. Set SNMP to only run on the 127.0.0.1 loop back interface and allow any additional trap destinations, which is for remote management. Use this procedure:

Step 1. From the Services applet in the Control Panel, choose **SNMP**.

Step 2. Click the **Security** tab. At the bottom, allow only requests from 127.0.0.1 and any additional IP trap destinations.

Note: The BBSM Hotspot appliance has this as the default setting.

8. Set ACL on router or PIX to only allow explicit access to port 1433 (SQL) from outside the network.
9. Set ACL on internal network to block TCP port 1433 and TCP port 1434 on the BBSM server IP addresses from internal network (if there is an appropriate aggregate device in a routed environment).
10. Force both NIC interfaces to 100 MB Full Duplex if your network supports it, and configure the connected switch/router interface ports to 100 MB/FD as well, if supported. (This requires a reboot later.) If you are connecting to a half duplex only or 10 MB device, force that accordingly.
11. Disable QoS Service on both network interfaces in the network Control Panel. (This requires a reboot later.)

Note: The BBSM Hotspot appliance has this as the default setting. Use this procedure:

Step 1. From the desktop, choose **My Computer > Control Panel > Network and Dial Up Connections**.

Step 2. Choose the External interface.

Step 3. Right-click **External**, and select **Properties**.

Step 4. Scroll down and uncheck the **QoS Packet Scheduler** check box.

Step 5. Click **OK**, and close the panel.

Note: Run through these steps again for the AtNatMP interface.

12. Disable NetBios over TCP/IP in the Advanced Tab for EACH network interface. Use this procedure:

Step 1. From the desktop, choose **My Computer > Control Panel > Network and Dial Up Connections**.

Step 2. Choose the External interface.

Step 3. Right-click **External**, and select **Properties**.

Step 4. Scroll down to Internet Protocol (TCP/IP) and select **Properties**.

Step 5. Click **Advanced**.

Step 6. Select the **WINS** tab.

Step 7. Select the **Disable NetBIOS over TCP/IP** radio button.

Step 8. Click **OK** through the prompts.

Note: Run through these steps again for the AtNatMP interface.

13. Set up the FTP service and disallow anonymous access. Use this procedure:

Step 1. Right click on the FTP site, and select **Properties**.

Step 2. Select the **Security Accounts** tab.

Step 3. Uncheck the **Allow Anonymous Connections** check box.

Note: The IIS Lockdown tool disables FTP service automatically. Disabling this will break the WEBpatch utility. Enable it when running WEBpatch and then disable again after patch upgrades.

14. Set the DHCP Service to only run on the internal NIC. Use this procedure:

Step 1. Choose **Start > Programs > Administrative Tools > DHCP**.

Step 2. Right-click on the BBSM server icon and select **Properties**.

Step 3. Select the **Advanced** Tab.

Step 4. Click **Bindings**.

Step 5. Uncheck the **External** check box.

Step 6. Restart the DHCP Service.

15. Set up boot time script to remove all shares. Use this procedure:

Step 1. Open Notepad.

Step 2. Copy and paste the following into the Notepad document:

```
@echo off
net share IPC$ /delete
net share C$ /delete
net share D$ /delete
net share mspclnt / delete
net share E$ /delete NOTE: your backup/image drive may be different!
net share ADMIN$ /delete
```

Step 3. Save the document as **deleteshares.cmd** in C:\atcom.

Step 4. Choose **Start > Run**.

Step 5. From the Run window, type **gpedit.msc** and click **OK**.

Step 6. Under Local computer Policy\Windows Settings, click **Scripts**.

Step 7. Right-click **Startup**, and click **Properties**.

Step 8. Click **Add**.

Step 9. Browse to c:\atcom\ and select **deleteshares.cmd**.

Step 10. Click **OK** and exit.

16. Harden the TCP/IP stack against DoS attacks in the registry.

Note: For this to take effect, you must reboot after completing all instructions in this document.

Note: We recommend that you back up your registry before modifying your registry settings. To back up the Windows registry, export the registry to a file. If there is a corruption, you can use the exported registry file to restore the settings.

To back up the registry, use this procedure:

1. Choose **Start > Run**. The Run window appears.
2. Enter **regedit**, and click **OK**. The Registry Editor window appears.
3. Double-click **HKEY_LOCAL_MACHINE**.
4. From the Registry menu, select **Export Registry File**.

5. Enter a file name, and click **Save**.

Registry Settings for Maximum Protection from Network Attack

The following registry settings will help to increase the resistance of the Windows 2000 network stack to network denial of service attacks.

RestrictAnonymous
Key: Hkey_Local_Machine\System\CurrentControlSet\Control\LSA
Value Type: REG_DWORD
Valid Range: 0, 1, 2

BBSM Setting: 2

New Key:

SynAttackProtect
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD
Valid Range: 0, 1, 2

BBSM Setting: 2

Add a DWORD value named SynAttackProtect.

Set the Value to 2.

New Key:

TcpMaxHalfOpen
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 100-0xFFFF
BBSM Setting: default 100, (64 in hex)

Add a DWORD value named TcpMaxHalfOpen.

Set the Value to 100 (64 in hex).

New Key:

TcpMaxHalfOpenRetried
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 80-0xFFFF
BBSM Setting: 80

Add a DWORD value named TcpMaxHalfOpenRetried.

Set the Value to 80 (in hex).

New Key:

TcpMaxPortsExhausted
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 0-65535
BBSM Setting: 5

Add a DWORD value named TcpMaxPortsExhausted.

Set the Value to 0x5 (hex).

New Key:

EnablePMTUDiscovery
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (False, True)
BBSM Setting: 0

Add a DWORD value named Enable PMTUDiscovery.

Set the Value to 0.

New Key:

NoNameReleaseOnDemand
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Netbt\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (False, True)
BBSM Setting: 1

Add a DWORD value named NoNameReleaseOnDemand.

Set the Value to 1.

New Key:

EnableDeadGWDetect
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Boolean
Valid Range: 0, 1 (False, True)
BBSM Setting: 0

Add a DWORD value named EnableDeadGWDetect.

Set the Value to 0.

New Key:

KeepAliveTime
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters
Value Type: REG_DWORD—Time in milliseconds
Valid Range: 1–0xFFFFFFFF
BBSM Setting: 300,000 (493E0 in HEX)

Add a DWORD value named KeepAliveTime.

Set the Value to 493E0 (in hex).

New Key:

PerformRouterDiscovery
Key: Hkey_Local_Machine\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\
Value Type: REG_DWORD
BBSM Setting: 0

Add a DWORD value named PerformRouterDiscovery.

Set the Value to 0.

Disable Kernel Paging

Key: Hkey_local machine\system\currentcontrolset\control\session manager\memory management\disblepagingexecutive

BBSM Setting: 1

Clear Paging File At Shutdown

Key: Hkey_local machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown

---

New Key:

Disable Media Sense on the network interfaces:

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Add a DWORD value named DisableDHCPMediaSense.

Set the value of DisableDHCPMediaSense to 1.

Close the Registry Editor and restart the computer.

Clear DHCP Database of Expired Leases:

Key:
HKEY_LOCAL_MACHINE\System\ControlSet001\Services\DHCPServer\Parameters\DatabaseCleanupInterval

BBSM Setting: 0000000a (10 minutes)

Set Windows Warning Logon Banner

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText

Type your warning message here.

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeCaption

BBSM Setting: "WARNING"

Do not Display Previously Used User Name:

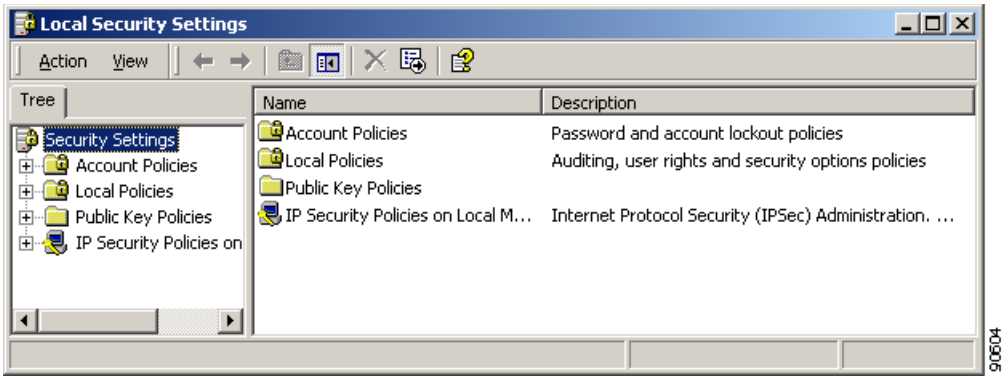
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisplay lastusername

---

17. Enable Auditing. Use this procedure:

Step 1. From the desktop, choose **Start > Programs > Administrative Tools > Local Security Policy.** The Local Security Settings window appears. (See Figure 1.)

Figure 1. Local Security Settings

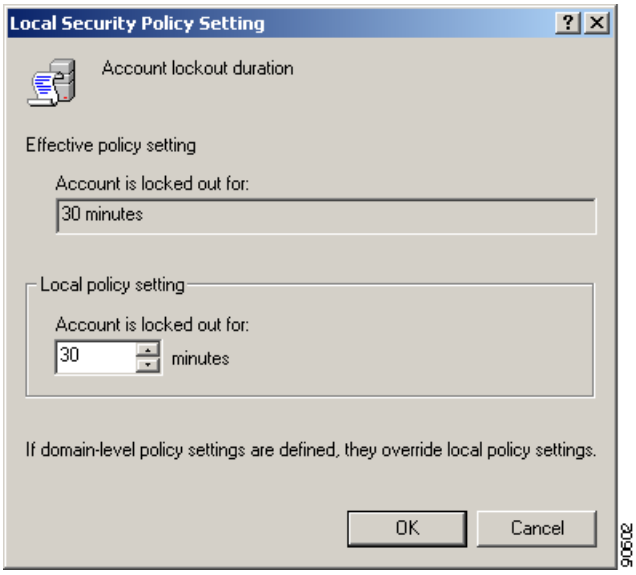


Step 2. From the left pane, click **Account Policies.**

Step 3. Double-click **Account Lockout Policy.**

Step 4. Double-click **Account lockout duration.** The Account lockout duration window appears. (See Figure 2.)

Figure 2. Account Lockout Duration



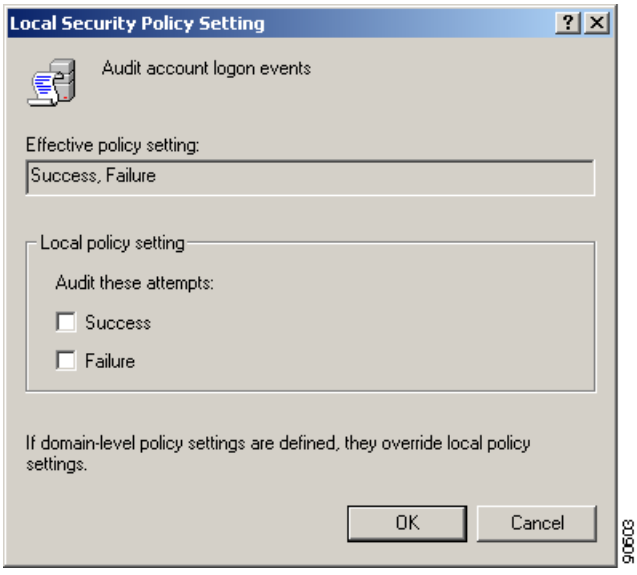
Step 5. From the drop-down menu, select **30** minutes, and click **OK.**

Step 6. From the Local Security Settings window, click **Local Policies.**

Step 7. Double-click **Audit Policy.**

Step 8. Double-click **Audit account logon events.** The audit account logon events window appears. (See Figure 3.)

Figure 3. Audit Account Logon Events



Step 9. Check the **Success** check box.

Step 10. Check the **Failure** check box.

Step 11. Click **OK.**

Step 12. Double-click **Audit account management.**

Step 13. Check the **Success** and **Failure** check boxes, and click **OK.**

Step 14. Double-click **Audit directory service access**.

Step 15. Verify that the Success and Failure check boxes are *not* checked (No Auditing) and click **OK**.

Step 16. Double-click **Audit logon events**.

Step 17. Check the **Success** and **Failure** check boxes, and click **OK**.

Step 18. Double-click **Audit object access**.

Step 19. Check the **Success** check box, and click **OK**.

Step 20. Double-click **Audit policy change**.

Step 21. Check the **Success** and **Failure** check boxes, and click **OK**.

Step 22. Double-click **Audit privilege use**.

Step 23. Check the **Success** and **Failure** check boxes, and click **OK**.

Step 24. Double-click **Audit process tracking**.

Step 25. Verify that the Success and Failure check boxes are *not* checked (No Auditing) and click **OK**.

Step 26. Double-click **Audit system events**

Step 27. Check the **Success** and **Failure** check boxes, and click **OK**.

Step 28. From the left pane of the Local Security Settings window, click **Security Options**.

Step 29. Double-click **Additional restrictions for anonymous connections**.

Step 30. From the Local policy setting drop-down menu, choose **No access without explicit anonymous permissions**.

Step 31. Click **OK**.

Step 32. Close the Local Security Settings window.

18. Increasing the NTFS Log Size. Use this procedure:

Step 1. From a cmd prompt, type **chkdsk c: /L:65536**.

Step 2. Click **Yes**.

19. Remove the OS/2 and Posix Subsystems.

Use the Registry Editor to remove the following registry entries:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE
Subkey: Microsoft\OS/2 Subsystem for NT
Entry: delete all subkeys
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\Environment
Entry: Os2LibPath
Value: delete entry
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Entry: Optional
Values: delete entry
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Values: Delete entries for OS/2 and POSIX
```

20. Remove the TsInternetUser Account

This account is not part of remote management Terminal server. It is used by Application Mode and not necessary here. Use this procedure to remove the TsInternetUser Account:

Step 1. From the desktop, choose **Start > Programs > Administrative Tools > Computer Management.** The Computer Management window appears.

Step 2. From the left pane, click **Local Users and Groups**.

Step 3. Double-click **Users**.

Step 4. Right-click **TsInternetUser**, and select **Delete**.

Step 5. Click **Yes**.

21. Install and run IISLockdown Tool.

Note: If IP Addressing is changed, you will have to run the IIS Lockdown tool two more time; once to remove settings, and again to enable them with the new IP settings.

Note: BBSM 5.2 SP1 will not install after the IIS Lockdown tool is applied. Install BBSM 5.2 SP1 prior to running the IIS Lockdown tool. If the IIS Lockdown tool is already installed, you need to uninstall it, run WEBpatch for BBSM 5.2 SP1, and then reinstall it.

Note: Once IIS is locked down by running the IIS lock-down tool, clients cannot connect if a domain name for SSL pages is enabled. IIS has to be unlocked first, and the server has to be rebooted in order to enable the domain name for SSL.

Use this procedure to Install and Run the Microsoft IIS Lockdown Tool:

Step 1. Using your web browser, go to this Microsoft website:

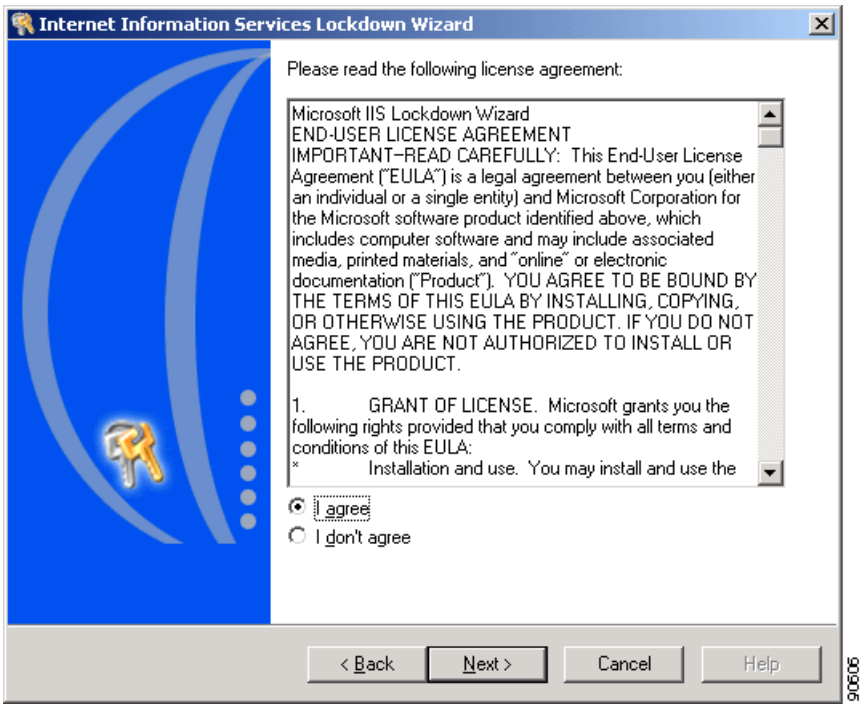
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp

Step 2. Download and open the IIS Lockdown Wizard. The Internet Information Services Lockdown Wizard appears. (See Figure 4.)

Figure 4. Internet Information Services Lockdown Wizard

Step 3. Click **Next**. The License Agreement appears. (See Figure 5.)

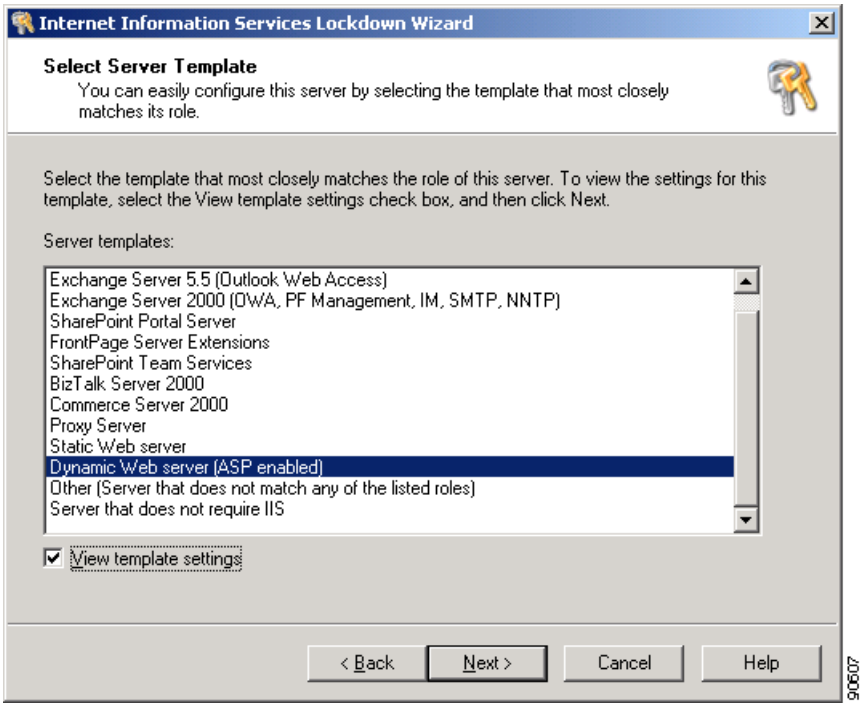
Figure 5. License Agreement



Step 4. Read the license agreement, and click the **I agree** radio button.

Step 5. Click **Next**. The Select Server Template window appears. (See Figure 6.)

Figure 6. Select Server Template

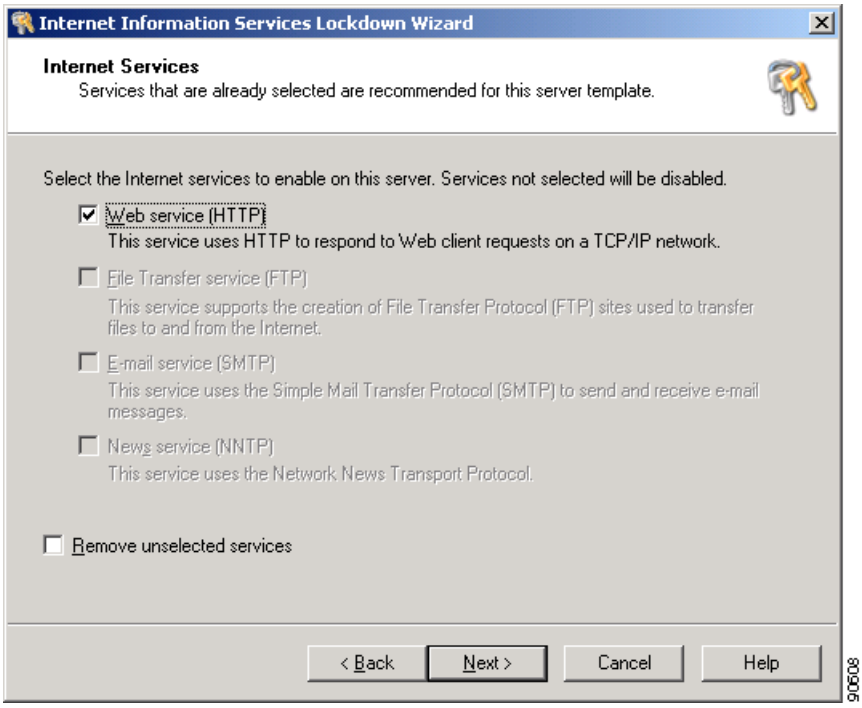


Step 6. Select **Dynamic Web server (ASP enabled)** and then check the **View template settings** check box.

Step 7. Click **Next**. The Internet Services window appears. (See Figure 7.)

Note: This is the only template that should be selected. Other choices will break the functionality of BBSM or expose the server unnecessarily.

Figure 7. Internet Services

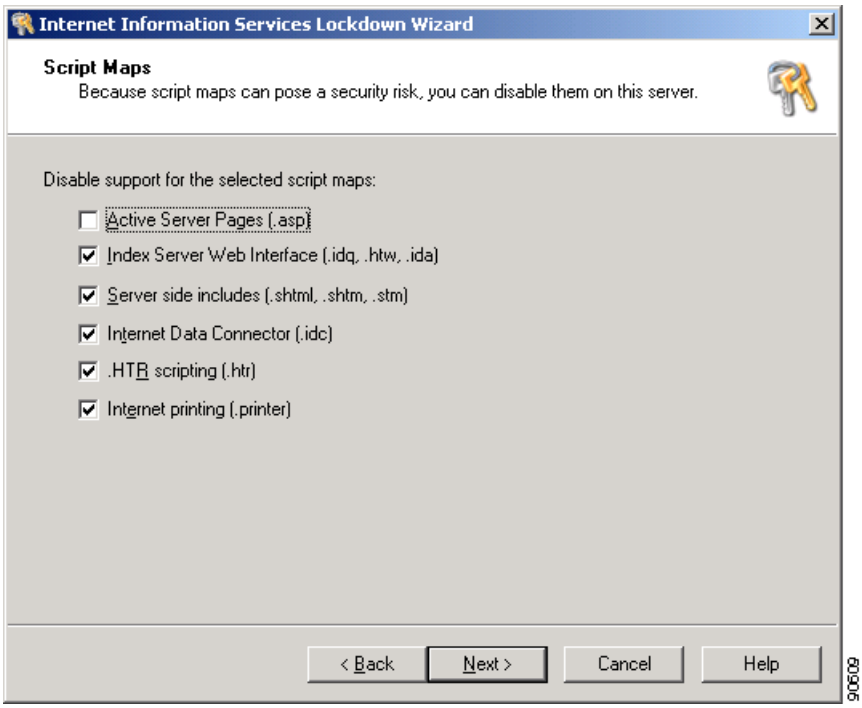


Step 8. Check only the **Web service (HTTP)** check box.

CAUTION: If FTP or any of the others are enabled, uncheck them. Do not check the Remove unselected services check box because you will need FTP for WEBpatch.

Step 9. Click **Next**. The Script Maps window appears. (See Figure 8.)

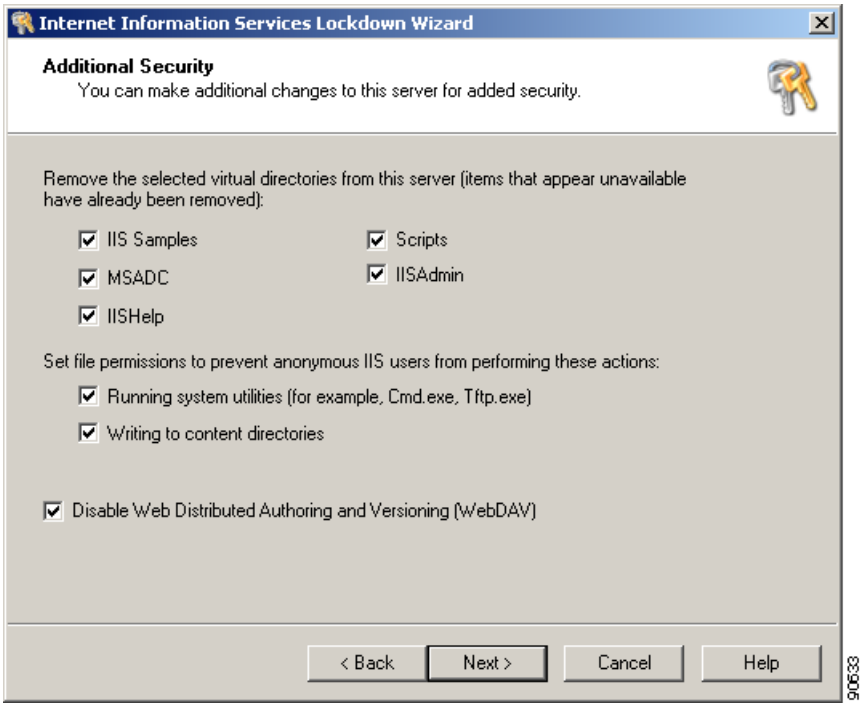
Figure 8. Scripts Maps



Note: All the check boxes should be checked except for Active Server Pages. Adding support for the other script mappings will expose the server. This is *not* recommended.

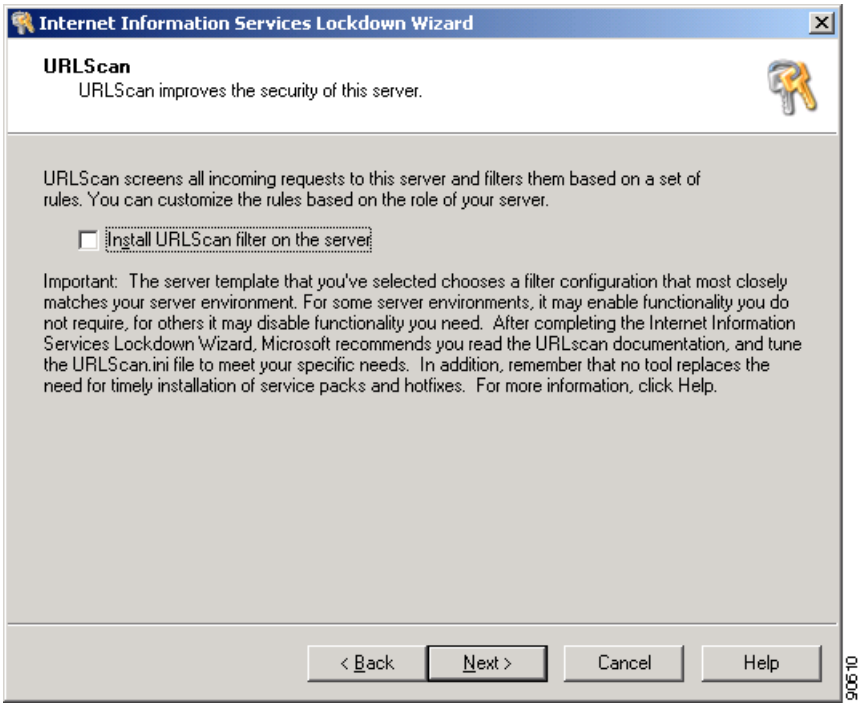
Step 10. Click **Next**. The Additional Security window appears. (See Figure 9.)

Figure 9. Additional Security



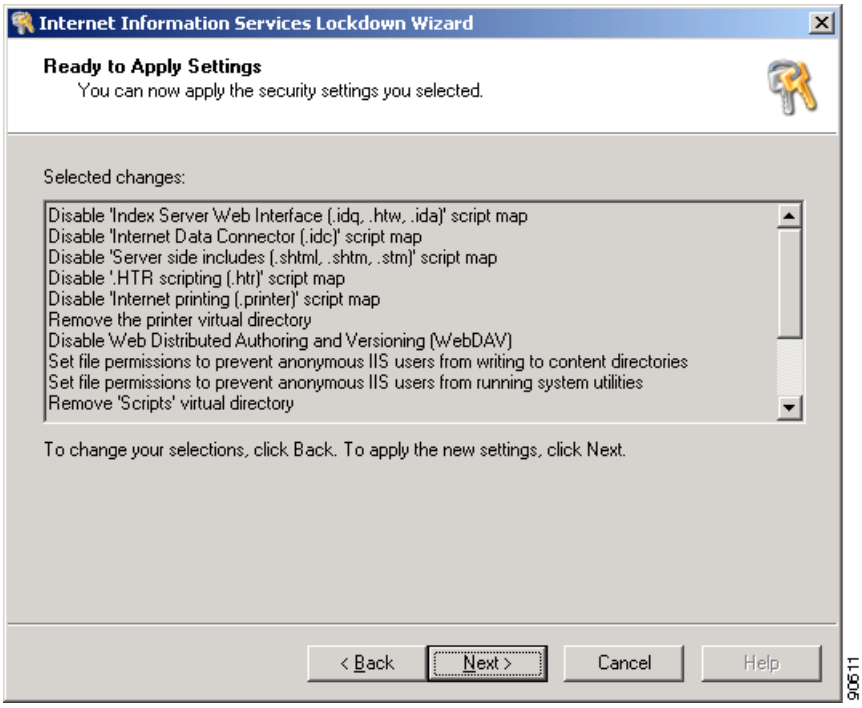
Step 11. Leave all of the check boxes checked, and click **Next**. The URLScan window appears. (See Figure 10.)

Figure 10. URLScan



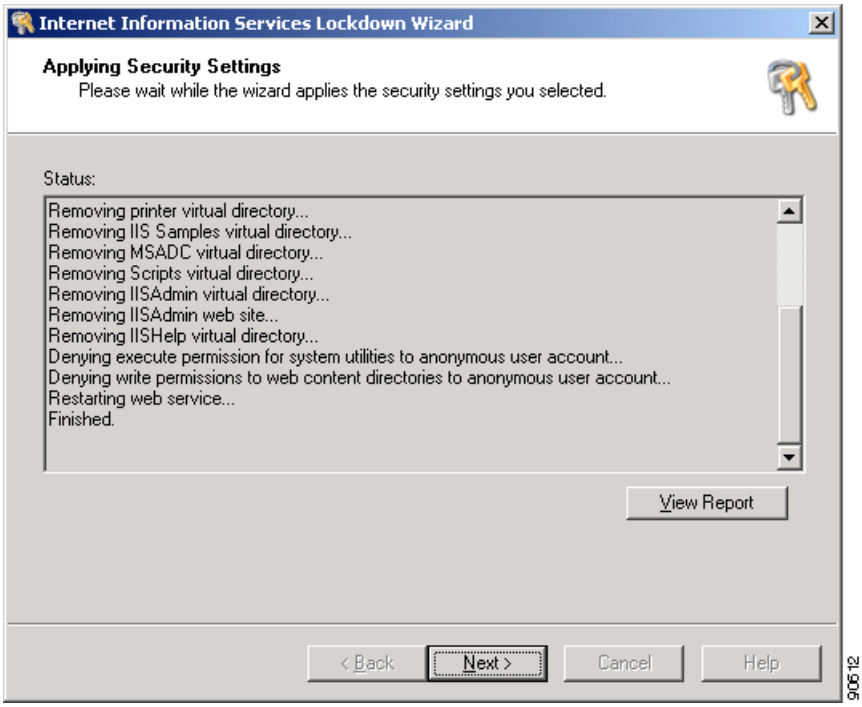
Step 12. Verify that the **Install URLScan filter on the server** check box is not checked, and click **Next.** (If it is checked, uncheck it.) The Ready to Apply Settings window appears. (See Figure 11.)

Figure 11. Ready to Apply Settings



Step 13. Click **Next.** Wait for the settings to be applied. The Applying Security Settings window appears. (See Figure 12.)

Figure 12. Applying Security Settings



Step 14. Click **Next.** The final page of the Internet Information Services Lockdown Wizard appears. (See Figure 13.)

Figure 13. Internet Information Services Lockdown Wizard

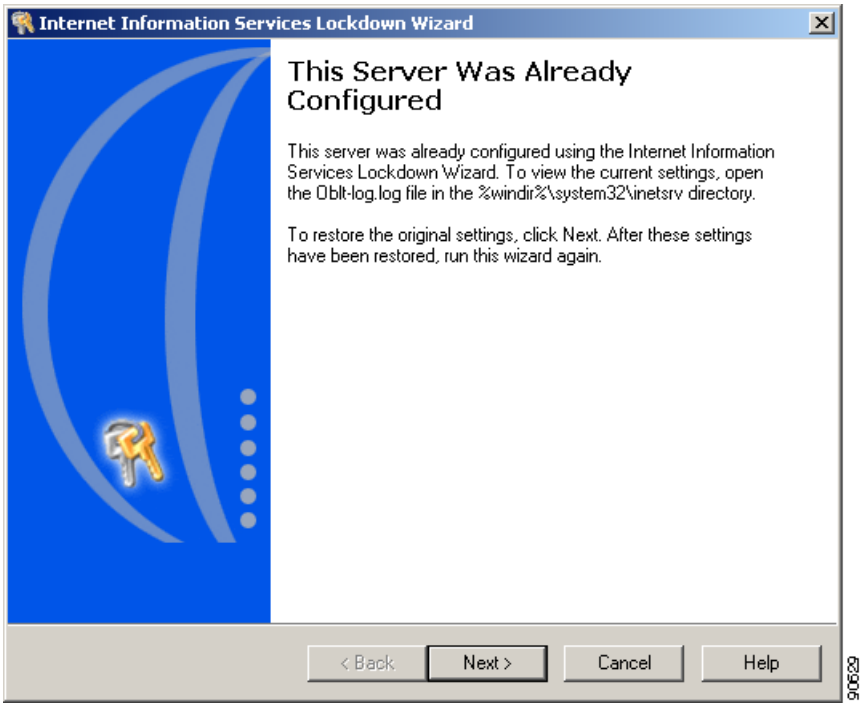
Step 15. Click **Finish**.

How to Uninstall the Lockdown Wizard

Use this wizard if you need to change IP addresses, if you are enabling SSL, or if you encounter other anomolies. You can safely run this wizard over again.

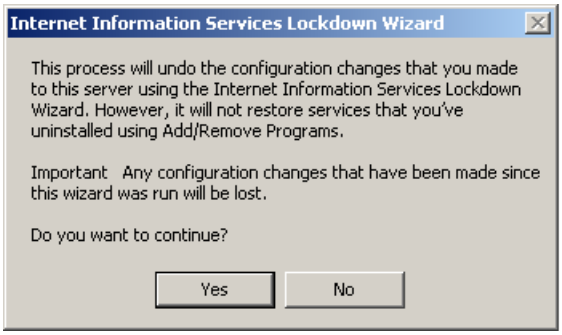
Step 1. Open the IIS Lockdown Wizard. The Server Was Already Configured window appears. (See Figure 14.)

Figure 14. This Server Was Already Configured



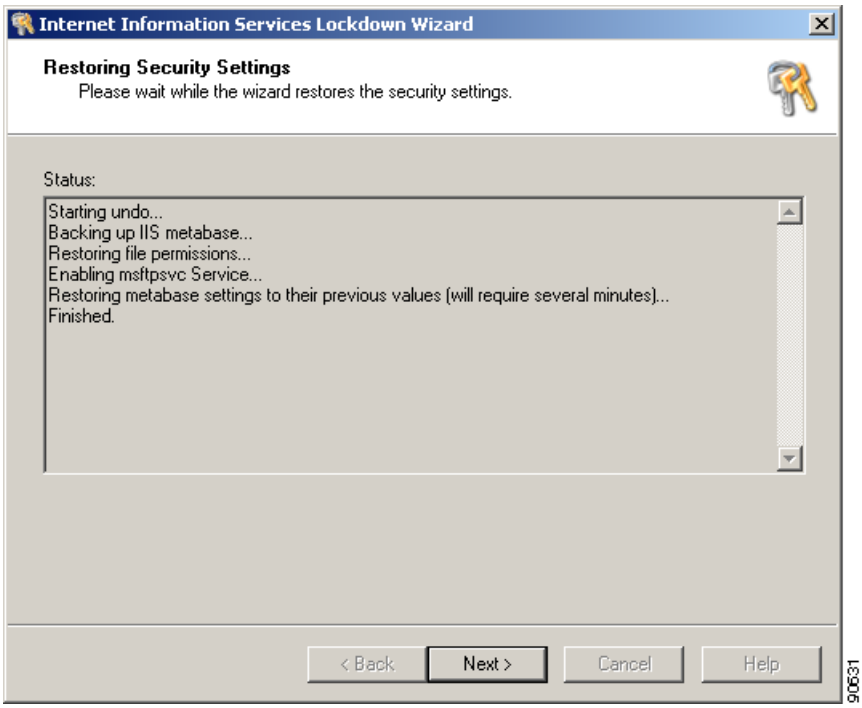
Step 2. Click **Next**. The Internet Information Services Lockdown Wizard appears. (See Figure 15.)

Figure 15. Internet Information Services Lockdown Wizard



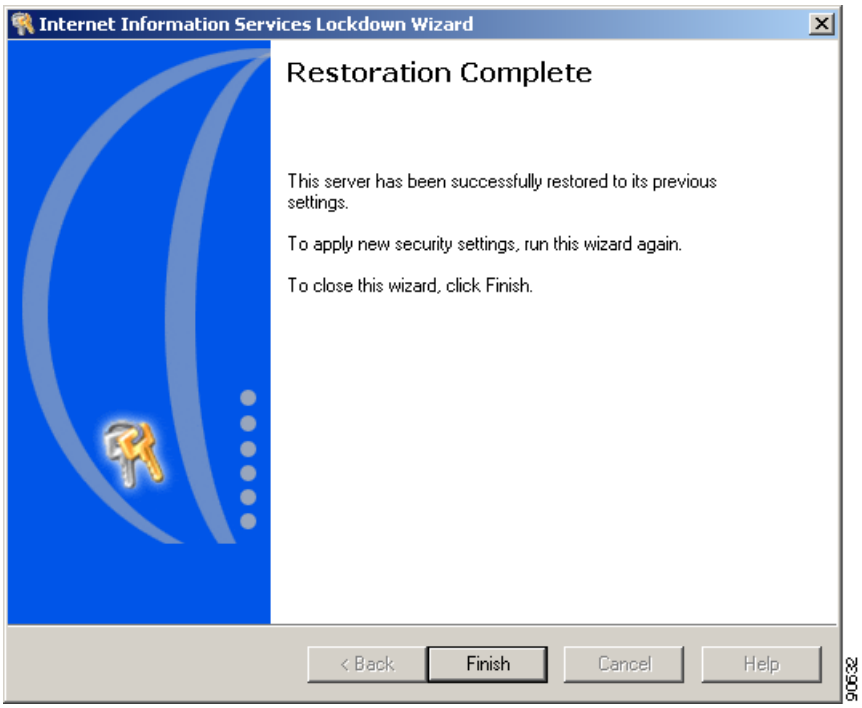
Step 3. Click **Yes**. The Restoring Security Settings window appears. (See Figure 16.)

Figure 16. Restoring Security Settings



Step 4. Click **Next**. The Restoration Complete window appears. (See Figure 17.)

Figure 17. Restoration Complete



Step 5. Click **Finish**.

Hardening Final Steps – Restricting IIS by IP Address Ranges

22. Restrict access to reporting and config pages except to explicit IP Addresses (no Internet Net, no internal network access). This is recommended.
23. Restrict access to all web pages to internal network range and to any external reporting or management IP addresses only:

Step 1. From the desktop, choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services window appears.

Step 2. From the left pane, click **bbsm**.

Step 3. Right-click **Default Web Site**, and select **Properties**.

Step 4. Select the **Directory Security** tab.

Step 5. From the IP address and domain name restrictions area, click **Edit**.

Step 6. Click the **Denied Access** radio button.

Step 7. Click **Add**.

Step 8. Click the **Single computer** radio button.

Step 9. In the IP address field, enter **127.0.0.1**, and click **OK**.

Step 10. Click **Add**.

Step 11. Enter the internal network's network ID and subnet mask, and click **OK**.

Step 12. If desired, click **Add** to enter any singular external network address, such as reporting, management, etc., and click **OK**. (This step is optional.)

Note: If prompted, select **ALL** on the Inheritance Overrides window, select the folder permissions in the Child Nodes window, and click **OK**. If you change the server IP addresses, you must change the ranges you just entered above to match the new addressing.

Note: If Multinet is configured after the above steps are completed, remember to add the second network to the list of networks that are granted access to Default Web Site in IIS.

24. Reboot the server now.

References and Related Documents:

- Internet Security Systems, Database Scanner Sample Reports, Policy, SQL Server, http://documents.iss.net/literature/DatabaseScanner/reports/sql/SQLPolicy.pdf
- Mark Lachniet Checklist
  http://www.mtip.net/aware/MarkLachnietChecklist.pdf
  Windows 2000 Security Technical Reference, Internet Security Systems, Inc. 2000, Microsoft Press.
- Microsoft Checklist for Windows Hardening,
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ security/lockdown.asp
- Securing Windows NT/2000 Server for the Internet, Stefan Norberg 2001, O'Reilly & Associates.
- SQL Server Auditing, John Howie, August 2002 issue of Security Administrator, posted on Microsoft Technet, http://www.microsoft.com/technet/security/prodtech/dbsql/sql2kaud.asp
- SQL 2000 C2 Admin and User Guide, Microsoft, 2 Nov 2000
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25503
- SQL Server 2000 Security White Paper
  http://www.microsoft.com/sql/techinfo/administration/2000/securityWP.asp
- SQLSecurity Checklist, http://www.sqlsecurity.com
- Threat Profiling Microsoft SQL Server (A Guide to Security Auditing), David Litchfield, 20th July 2002,
  http://www.ngssoftware.com
  http://www.nextgenss.com/papers/tp-SQL2000.pdf
- Windows 2000 Server Operating System Level 2 Benchmark Consensus Baseline Security Settings, 2002, The Center For Internet Security, Jeff Shawgo Editor.
- Windows 2000 Server Security, Thomas Shinder et al, 2000, Syngress Publishing.
- Windows 2000 TCP/IP Protocols and Services Technical Reference, Thomas Lee and Joseph Davies, 2000, Microsoft Press.

OBTAINING TECHNICAL ASSISTANCE

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services that help you:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to this website:

http://www.cisco.com.

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No work around is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No work around is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this website:

http://www.cisco.com/tac

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe