

## IIS 6.0 Security Checklist

This checklist should be utilized to help secure an IIS 6.0 web server.

### Patches and Updates

- Microsoft Baseline Security Analyzer is run on a regular interval to check for latest operating system and components updates
- The latest updates and patches are applied for Microsoft® Windows® operating system, IIS server, and the Microsoft .NET Framework.
- Subscribe to the Microsoft Security Notification Service

### IISLockdown

- IISLockdown has been run on the server
- URLScan is installed and configured

### Services

- Unnecessary Windows services are disabled.
- Services are running with least-privileged accounts
- FTP, SMTP, and NNTP services are disabled if they are not required
- Telnet service is disabled
- ASP.NET state service is disabled and is not used by your applications

### Protocols

- WebDAV is disabled if not used by the application OR it is secured if it is required. For more information, see Microsoft Knowledge Base article 323470
- TCP/IP stack is hardened.
- NetBIOS and SMB are disabled (closes ports 137, 138, 139, and 445).

### Accounts

- Unused accounts are removed from the server
- Windows Guest account is disabled.
- Administrator account is renamed and has a strong password
- IUSR\_MACHINE account is disabled if it is not used by the application
- If your applications require anonymous access, a custom least-privileged anonymous account is created
- The anonymous account does not have write access to Web content directories and cannot execute command-line tools
- ASP.NET process account is configured for least privilege. (This only applies if you are not using the default ASPNET account, which is a least-privileged account.)
- Strong account and password policies are enforced for the server
- Remote logons are restricted. (The "Access this computer from the network" user-right is removed from the Everyone group.)
- Accounts are not shared among administrators
- Null sessions (anonymous logons) are disabled

- Approval is required for account delegation
- Users and administrators do not share accounts
- No more than two accounts exist in the Administrators group
- Administrators are required to log on locally OR the remote administration solution is secure

### Files and Directories

- Files and directories are contained on NTFS volumes.
- Web site content is located on a non-system NTFS volume
- Log files are located on a non-system NTFS volume and not on the same volume where the Web site content resides
- The Everyone group is restricted (no access to \WINNT\system32 or Web directories).
- Web site root directory has deny write ACE for anonymous Internet accounts
- Content directories have deny write ACE for anonymous Internet accounts
- Remote IIS administration application is removed (\WINNT\System32\Inetsrv\IISAdmin).
- Resource kit tools, utilities, and SDKs are removed
- Sample applications are removed (\WINNT\Help\IISHelp, \Inetpub\IISamples).

### Shares

- All unnecessary shares are removed (including default administration shares).
- Access to required shares is restricted (the Everyone group does not have access).
- Administrative shares (C\$ and Admin\$) are removed if they are not required (Microsoft Management Server (SMS) and Microsoft Operations Manager (MOM) require these shares).

### Ports

- Internet-facing interfaces are restricted to port 80 (and 443 if SSL is used).
- Intranet traffic is encrypted (for example, with SSL) or restricted if you do not have a secure data center infrastructure

### Registry

- Remote registry access is restricted
- SAM is secured (HKLM\System\CurrentControlSet\Control\LSA\NoLMHash).

### Auditing and Logging

- Failed logon attempts are audited
- IIS log files are relocated and secured
- Log files are configured with an appropriate size depending on the application security requirement
- Log files are regularly archived and analyzed
- Access to the Metabase.bin file is audited

- IIS is configured for W3C Extended log file format auditing

### **Sites and Virtual Directories**

- Web sites are located on a non-system partition
- "Parent paths" setting is disabled
- Potentially dangerous virtual directories, including IISamples, IISAdmin, IISHelp, and Scripts virtual directories, are removed
- MSADC virtual directory (RDS) is removed or secured
- Include directories do not have Read Web permission
- Virtual directories that allow anonymous access restrict Write and Execute Web permissions for the anonymous account
- There is script source access only on folders that support content authoring
- There is write access only on folders that support content authoring and these folder are configured for authentication (and SSL encryption, if required).
- FrontPage Server Extensions (FPSE) are removed if not used. If they are used, they are updated and access to FPSE is restricted

### **Script Mappings**

- Extensions not used by the application are mapped to 404.dll (.idq, .htw, .ida, .shtml, .shtm, .stm, .idc, .htr, .printer).
- Unnecessary ASP.NET file type extensions are mapped to "HttpForbiddenHandler" in Machine.config

### **ISAPI Filters**

- Unnecessary or unused ISAPI filters are removed from the server

### **IIS Metabase**

- Access to the metabase is restricted by using NTFS permissions (%systemroot%\system32\inetsrv\metabase.bin).
- IIS banner information is restricted (IP address in content location disabled).

### **Server Certificates**

- Certificate date ranges are valid
- Certificates are used for their intended purpose (for example, the server certificate is not used for e-mail).
- The certificate's public key is valid, all the way to a trusted root authority
- The certificate has not been revoked

### **Machine.config**

- Protected resources are mapped to HttpForbiddenHandler
- Unused HttpModules are removed
- Tracing is disabled.  
<trace enable="false"/>

- Debug compiles are turned off.  
`<compilation debug="false" explicit="true" defaultLanguage="vb">`

#### **Code Access Security**

- Code access security is enabled on the server.
- All permissions have been removed from the local intranet zone.
- All permissions have been removed from the Internet zone.

#### **Other Check Points**

- IISLockdown tool has been run on the server.
- HTTP requests are filtered. URLScan is installed and configured.
- Remote administration of the server is secured and configured for encryption, low session time-outs, and account lockouts

