

## Windows Server 2003, Enterprise Edition Security Checklist

This checklist will help to secure newly installed Windows Server 2003 member server.

- Verify that all disk partitions are formatted with NTFS
- Verify that the Administrator account has a strong password
- Disable unnecessary services
- Disable or delete unnecessary accounts
- Protect files and directories
- Make sure the Guest account is disabled
- Protect the registration from anonymous access
- Apply appropriate registry ACLs
- Restrict access to public Local Security Authority (LSA) information
- Set stronger password policies
- Set account lockout policy
- Configure the Administrator account
- Revoke the Debug programs user right
- Remove all unnecessary file shares
- Set appropriate ACLs on all necessary file shares
- Enable security event auditing
- Set log on warning message
- Install anti-virus software and updates
- Install service packs and critical patches
- Automate patch deployment
- Scan system with the Baseline Security Analyzer
- Additional security settings
- Install the latest Service Pack
- Install the appropriate post-Service Pack security hotfixes

For better security, the Windows Server 2003 Security Configuration Wizard can also be used to harden the security of the server.

First, a security policy must be created.

- Click **Start**, click **Administrative Tools**, and then click **Security Configuration Wizard**.
- Read the Welcome page and click **Next**.
- Select “**Create a new security policy**” and then click **Next**.
- Type the name of the prototype server and then click **Next**.
- Wait for the Security Configuration Database to be processed, and then click **Next**.

- On the **Role-Based Service Configuration** page, click **Next**.
- On the **Select Server Roles** page, click **Next**.
- On the **Select Client Features** page, click **Next**.
- On the **Select Administration and Other Options** page, click **Next**.
- On the **Select Additional Services** page, click **Next**.
- On the **Handling Unspecified Services** page, click **Next**.
- On the **Confirm Service Changes** page, click **Next**.
- On the **Network Security** page, click **Next**.
- On the **Open Ports and Approve Applications** page, click **Next**.
- On the **Confirm Port Configuration** page, click **Next**.
- On the **Registry Settings** page, click **Next**.
- On the **Require SMB Security Signatures** page, click **Next**.
- On the **Require LDAP Signing** page, click **Next**.
- On the **Outbound Authentication Methods** page, click **Next**.
- On the **Outbound Authentication Using Domain Accounts** page, click **Next**.
- On the **Registry Settings Summary** page, click **Next**.
- On the **Audit Policy** page, click **Next**.
- On the **System Audit Policy** page, click **Next**.
- On the **Audit Policy Summary** page, click **Next**.
- On the **Internet Information Services** page, click **Next**.
- On the **Select Web Service Extensions for Dynamic Content** page, click **Next**.
- On the **Select Virtual Directories to Retain** page, click **Next**.
- On the **Prevent Anonymous Users from Accessing Content Files** page, click **Next**.
- On the **IIS Settings Summary** page, click **Next**.
- On the **Save Security Policy** page, click **Next**.
- On the **Security Policy File Name** page, type a name for the prototype policy, and then click **Next**.  
Do not name the security policy by using the name of the prototype computer because scwcmd.exe uses *computername.xml* to save analysis results, and you do not want the security policy to have the same name as the analysis results. That would risk confusion or overwriting.
- On the **Completing the Security Configuration Wizard** page, click **Finish**.

Once the security policy is created, it can then be applied to the server.

- Click **Start**, click **Administrative Tools**, and then click **Security Configuration Wizard**.
- Read the Welcome page and click **Next**.
- On the **Configuration Action** page, select **Apply an existing security policy**, type in the full path and file name of the policy, and then click **Next**.
- On the **Select Server** page, type in the name of the server to which the policy will be applied and then click **Next**. On the **Apply Security Policy** page, click **Next**.

- On the **Applying Security Policy** page, wait for processing to finish, and then click **Next**.
- On the **Completing the Security Configuration Wizard** page, click **Finish**.

