Windows 2003, Windows 2008, Windows 2012 and Windows 2016 Server Security Standard

RIJAKUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division

1.0 Introduction

1.1 Objective(s)

1.1.1 To specify a baseline configuration for implementations of Microsoft Windows 2003, Windows 2008, Windows 2012 and Windows 2016 Server.

1.1.2 To provide guidance to administrators, developers and security personnel in securely implementing Microsoft Windows 2003, Windows 2008, Windows 2012 and Windows 2016 Server.

1.2 Scope

1.2.1 All of the Organization's Microsoft Windows 2003, Windows 2008, Windows 2012 and Windows 2016 Server systems will be subject to the policies specified within this security standard. The policies will be applied to new and existing installations.

1.3 Definitions

NTFS

Short for **NT** **F**ile **S**ystem, one of the file systems for the Windows NT operating system. NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files.

ASCII

Acronym for **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange. ASCII is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127.

FTP

Short for **F**ile **T**ransfer **P**rotocol, the protocol for exchanging files over the Internet.

IIS

Short for **I**nternet **I**nformation **S**erver, Microsoft's Web server that runs on Windows NT platforms.

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division

SMTP

Short for **S**imple **M**ail **T**ransfer **P**rotocol, a protocol for sending e-mail messages between servers.

WWW

A system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files.

SNMP

Short for **S**imple **N**etwork **M**anagement **P**rotocol, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network

2.0 Installation and Configuration

2.1 Verify that all Disk Partitions are Formatted with NTFS

2.1.1 Ensure that all partitions on your server are formatted using NTFS. NTFS partitions offer better access controls and protections.

2.2 Verify that the Administrator Account has a Strong Password

2.2.1 For maximum protection, ensure that the Administrator account password is at least 7 characters long and that it includes at least one punctuation mark or non-printing ASCII character (ALT key and three-digit key codes on the numeric keypad). (Ref: Section 2.9)

2.2.2 The Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

2.3 Disable Unnecessary Services

2.3.1 Disable any network services not required for the computer. In particular, disable the following services if possible:

- (Internet Information Server) IIS services:
  - FTP Publishing Service
  - IIS Admin Service
  - Network News Transport Protocol (NNTP)
  - Simple Mail Transport Protocol (SMTP)
  - World Wide Web Publishing Service

- Server service
  - Disable if server is not being used for file and print sharing.

- SNMP service
  - Disable if SNMP monitoring if not required.

2.3.2 Avoid installing applications on the server unless they are absolutely necessary to the server's function.

2.4 Disable or Delete Unnecessary Accounts

2.4.1 Review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, and disable any non-active accounts, and delete accounts that are no longer required.

2.5 Ensure the Guest Account is Disabled

2.5.1 By default, the Guest account is enabled on systems running Microsoft Windows 2003, Windows 2008, Windows 2012 and Windows 2016 Server. If the Guest account is enabled, disable it.

2.6 Set Stronger Password Policies

2.6.1 Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance.

2.6.1.1 Set the minimum password length to at least 7 characters.

2.6.1.2 Set a minimum password age to 3 days.

2.6.1.3 Set a maximum password age to 60 days.

2.6.1.4 Set password history maintenance (using the "**Remember passwords**" option) of at least 5.

2.6.1.5 Set a password complexity requirement (using the **Passwords must meet complexity requirements** option.

2.7 Set Account Lockout Policy

2.7.1 Enable lockout: 5

2.7.2 Reset count after: 30 minutes

2.7.3 Set lockout duration: 30 minutes

2.8 Remove all Unnecessary File Shares

2.8.1 All unnecessary file shares on the system must be removed to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system. (Ref: Section 2.5)

2.9 Set Appropriate ACLs on all Necessary File Shares

2.9.1 All shares that are required on the system should have the ACL restricted such that users have the appropriate share-level access. (Ref: Section 3.0)

2.10 Enable Security Event Auditing

2.10.1 Enable **Success** and **Failure** auditing for the **Audit account logon events** policy.

2.10.2 Maximum security log size be set to a value of 184,320 KB.

2.10.3 Maximum application log size be set to 10,240 KB.

2.10.4 Maximum system log size to 10,240 KB.

2.10.5 Set the retention method for event logs to **Overwrite events as needed**.

2.11 Set Log on Warning Message

2.11.1 Set message text for users attempting to log on to the following message value:

This system is restricted to authorized users.

Individuals attempting unauthorized access will be penalized.

If unauthorized, terminate access now!

Clicking on OK indicates your acceptance of the information in the background.

2.11.2 Set message title for users attempting to log on to:

IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORISATION.

2.12 Install Antivirus Software and Updates

2.12.1 Install anti-virus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems.

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division

2.13 Install Service Packs and Critical Patches

2.13.1 Apply all service packs and critical updates listed for your system at the Windows Update site. Before deploying on production servers, ensure that the patches are fully tested in a development environment.

3.0 Privileges

3.1 Restrict access to login scripts and profiles if possible.

3.2 The advanced user right to logon as a service must be assigned only to administrators.

3.3 The advanced user right to profile system performance must be assigned only to administrators.

3.4 The advanced user right to increase scheduling priority must be assigned only to administrators.

3.5 The advanced user right to act as part of the operating system must be assigned to no one.

3.6 The advanced user right to create permanent shared objects must not be assigned to any users.

3.7 The advanced user right to create a token object must not be assigned to any users.

3.8 The user right to logon locally should be assigned to local groups and not to individual users.

3.9 The advanced user right to create a page file must not be assigned to any users.

3.10 The advanced user right to replace a system level process token must be assigned to no user.

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division

3.11 The advanced user right to profile single process must be assigned only to administrators.

3.12 The user right to force shutdown from a remote system should be assigned to local groups and not to individual users.

3.13 The advanced user right to modify firmware environment variables must be assigned only to administrators.

3.14 The user right to shutdown the system should be assigned to local groups and not to individual users.

3.15 The advanced user right to load and unload device drivers must not be assigned to any users.

3.16 The user right to change the system time should be assigned to local groups and not to individual users.

3.17 The advanced user right to generate security audits must not be assigned to any users other than administrators or security teams.

3.18 The user right to backup files and directories must only be held by Backup Operators.

3.19 The advanced user right to increase quotas must be held by administrators only.

4.0 Network Security

4.1 Remote Access Server (RAS) must be enabled only if required.

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division

5.0 Events to Be Audited

5.1 Set up auditing for the following events

Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Success, failure
Policy change	Success, failure
Privilege use	Success, failure
Process tracking	Success, failure
System events	Success, failure

RIJALUDDIN SALLEH
Senior General Manager, Head
Group Compliance & General Services Division