Orchestrating a brighter world

NEC

NEC Group Internal Use Only

NEC Intranet Windows Server Security Enhancement Guide

July 19, 2016
Version 2.00

Security Technology Center
Management Information Systems Division
NEC Corporation

Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.

改版履歴

Date	Ver.	Description
Sep. 28, 2012	1.0	First version created.
Jul. 03, 2013	1.1	Notes added for users not to use the values shown in the Secure Server Construction Guide Series directly. • A note added to P10 “Reference Guides” in “Glossary (2/2)”. • Each page from 2.1 to 2.4, added a message saying ”Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.”
Jul. 19, 2016.	2.0	To respond to advanced targeted attacks, countermeasures against them modified.

Contents

1. Introduction

2. Measures to Enhance Security
 2.1 Strengthening Authentication
 2.2 Mitigating Vulnerabilities
 2.3 Strengthening Network Security
 2.4 Strengthening Operation Security

3. Reference

1. Introduction

About This Document

This document is created to indicate security measures for Windows servers on the intranet to cope with cyber attacks that are getting more and more sophisticated.

Recently, the number of targeted attacks in which the attacker targets a specific target (usually people working at a specific company or organization) in an attempt to steal confidential information or access privileges in the corporate network is increasing.

This guide is created to enhance security for protecting our Windows servers against these advanced cyber attacks.

We believe this guide will help all administrators of the NEC Group improve the security level of their Windows servers furthermore.

If you have any questions about this document, contact:

Security Technology Center (STC)
Management Information Systems Division, NEC Corperation
E-mail to: c-tiger-faq@cit.jp.nec.com

Target Scope of This Document (1 / 2)

Target scope of this document is as follows:

◆ Scope of the target servers

- Windows servers located on the NEC Intranet
- Note that the most measures described here are for Operation Systems. Measures for applications have to be considered by organization independently.

◆ Intended audience of this document

- Windows server developers
- Windows server administrators and operators

◆ Details differ depending on the server's situation

- For Windows servers currently being located on the NEC Intranet:
  Measures described here have to be completed by the due date after responsible people confirm the details.
- For Windows servers scheduled to be newly located on the NEC Intranet:
  Security measures described here have to be implemented.
- For Windows server located or scheduled to be located on customers' network
  Confirm measures described in this document and conclude an agreement with the customer on security measures to be taken for the server.

Note that the measures shown in this document are required minimum to defend advanced cyber attacks, and cannot block all the cyber attacks. But implementing these measures will help you detect attacks in the early stage, resulting in only limited damage to your environment.

2. Measures to Enhance Security

Glossary (1 / 2)

Terms used in this Section 2 are defined as follows.

Requirement level

- Security measures are classified into three levels based on the requirement scope:
  - **Mandatory;**
    Measures equal to those described in the “NEC Intranet Technology and Management Rules”.
  - **Mandatory (limited);**
    Measures required to be implemented in principle for systems whose Security Level is 3 or greater* except for the case implementing them may affect the services/operations. These measures are planned to become standards of “NEC Intranet Technology and Management Rules”. (Note that even if these measures become corporate standards, there will be a certain period of tim to prepare for actual implementation.) For systems whose Security Level is 2 or lower, it is required to implement all Mandatory measures without fail, while measures ranked as “Mandatory (limited)” remain as recommended status.
  - **Recommended;**
    Measures to be implemented if necessary for blocking targeted attacks.

Recommended value

- A baseline value is recommended by MIS Tokyo for implementing each measure. In principle, the recommended values must be followed in all environments except for those in which following the recommendation will affect services/operations or you cannot change the settings because you are participating in NEC Group’s ZENSYA Windows Domain System (“nsl domain”). Even if you are joining the nsl domain, you are required to review your security measures for smooth service operations as security measures of the nsl domain may be strengthened to the level of recommended values.

*For more details, see Standards for Implementing Secure Development and Operations at
http://www.mspd.nec.co.jp/security/secdev/standard/secdev_std.html (Japanese)
http://sec.zpf.nec.co.jp/security/gsecdev/standard/secdev_std.html (English)

Note that even if your system’s Security Level is temporarily deemed as Level 2 because it is not connected to any external network, the system must be considered as the target of “Mandatory (limited)” measures.

Glossary (2 / 2)

Reference guides

- Listed below are guides to be referenced in setting up your servers to implement measures.
  - Secure Development and Operations
    http://sec.zpf.nec.co.jp/security/gsecdev/guide.html

Note that the values recommended in the above guides must not be applied directly to your systems as they are values for Internet servers. Please use these guides for:

- Confirming how to set up and apply values recommended in this guide to your servers
- Information in determining values to be set up because this guide does not recommend specific values for some measures (#4-(1), for example) since appropriate values differ depending on conditions of the server.

For information only
2K3: **Secure Server Building Guide (Windows Server 2003)**
(http://www.mspd.nec.co.jp/security/secdev/download/STCIRT-W2K3.html)

Targeted Attacks: How Attackers Try to Break In and How to Prevent It

In targeted attacks, attackers often obtain passwords on operation terminals and use them with Administrative Shares and/or Task Scheduler to break into servers.

Effective Security Measures

1. Security measures for operation terminals

- Operation terminals must be dedicated to operation (They should not be used as a business PC.)

2. Security measures for servers/operation terminals

- Restrict the use of Administrative Shares.
- Restrict the use of Task Scheduler.
- Avoid using Active Directory when it is possible. If using Active Directory is indispensable, implement measures to keep the security level.
- Do not use the same password as is used for other machine(s).

Targeted Attacks and Counter measures against Them

In targeted attacks, attackers often use protocols such as TCP, UDP, ICMP and DNS to communicate with a relay server that has been placed independently in the intranet. Sometimes P2P technology is used as well.

Effective Security Measures

1. Restrict destination of the traffic from servers/operation terminals

- In principle, prohibit all communications between servers and operation terminals: permit only communications that are required for operating the system.
- Use firewalls to restrict traffic. Filter communications between them **mutually.** If it is difficult to prepare firewall equipment anytime soon, you may use personal firewalls for the time being.
- Even if communication is permitted, the **IP addresses of the destination must be restricted.**
- If communication is permitted, **alternative measures to mitigate risks** must be implemented.
- The logs must be checked on a regular basis.

Using Active Directory

Using an Active Directory (AD) will reduce the security level because enable multiple servers to share credentials. Avoid using an Active Directory wherever possible.

Effective Security Measures

1. Avoid using AD when it is possible

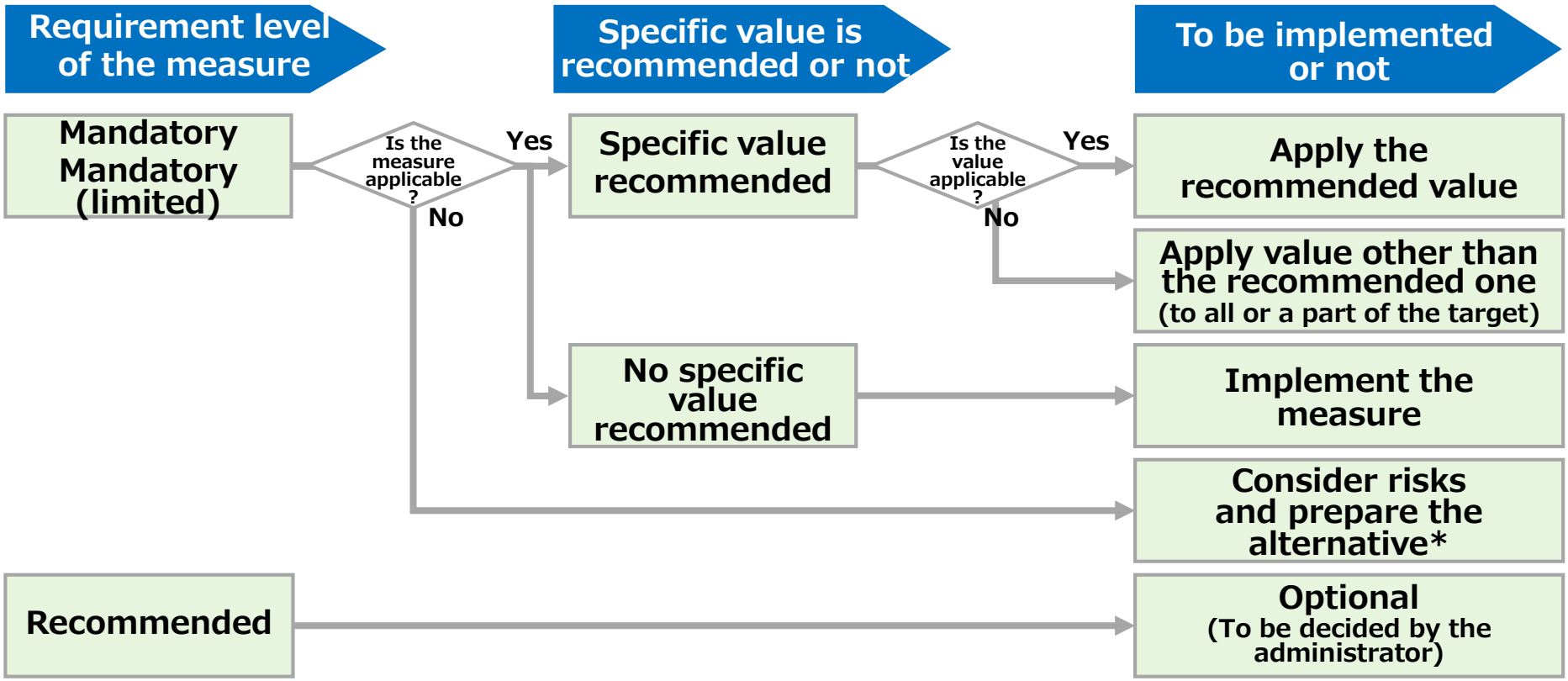
- Refrain from using AD when it is possible.

2. If it is required to use AD, measures to reduce risks must be implemented.

- Minimize the number of accounts to which Administrator privileges are granted.
- Administration tasks must be operated with a local account (for avoiding credentials to be shared).
- Set security policies of AD servers to reach the required security level.
- Monitor and check log records strictly.
- Restrict traffic destinations with IP addresses.

Criteria to Judge whether you should implement the measure

Implementation Judgement flow



*When implementing “Mandatory (limited)” measures or changing the setting to the “Recommended value” will affect your services/operations, please consult with the people responsible for the service, identify possible risks and then conduct alternative security measures or set an appropriate value.

2.1 Strengthening Authentication

Enhance administrator/operator authentication to prevent ID spoofing/thefts.

No	Security Measures	Requirement Level	Recommended value	Remarks
1	**Server administrators/operators must use a strong password.** Reduce threats of password analysis by using **Password Policy**, **Security Options** and other security settings to prohibit a weak password from being created. ➢ Set the minimum length for a password. ➢ Set the effective period for a password. ➢ Restrict using a too simple password. ➢ Restrict sharing a single password. ➢ Restrict using an account without setting a password for it. Note, however, that in the following cases, the administration team must add some complementary means to operations to keep the strength of passwords meeting the required security level: ➢ You cannot apply a single policy to all local accounts.	**Mandatory**	See 3.1	
2	**Set account lockout thresholds for server administrators/operators accounts.** To prevent ID spoofing, set account lockout thresholds as follows by using **Account Lockout Policy**. ➢ Lock out an account for a certain period when the user failed to pass the authentication more than a certain number of times. Note, however, that you cannot set account lockout threshold by yourself in the following case:	**Mandatory**	See 3.2	
3	**Restrict the use of built-in Administrator accounts.** Select one of the following measures by using **Security Options** to prevent attackers from stealing default built-in Administrator accounts placed in Windows OS ➢ Disable the built-in Administrator ➢ Rename the built-in Administrator	Recommended	See 3.3	

Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.

2.2 Mitigating Vulnerabilities (1/2)

To respond to attacks exploiting vulnerabilities, implement measures on servers to mitigate the vulnerabilities.

No.			Security Measures	Requirement Level	Recommended value	Remarks
4	(1)		**All the unnecessary services must be deleted; if there is a service difficult to be deleted, disable it.**	**Mandatory**	-	
			To mitigate attacks exploiting vulnerabilities, set up servers to run only services they needed on them.			
	(2)		**Implement measures to prevent buffer overflow attacks.**			
		a)	Use **Enable Data Execution Prevention (DEP)** to mitigate risks of buffer overflow attacks.	**Mandatory**	See 3.5	
		b)	To mitigate risks of buffer overflow attacks, use a tool such as **EMET** for monitoring memory status to prevent attacks that exploit vulnerabilities.	Recommended	-	Before actually using **EMET**, you must validate that there is no problem in running it.
	(3)		**Restrict the use of executable applications.**	Recommended	-	You can use **AppLocker** on Windows Server 2008 R2 or later only.
			Identify which applications are required by the server and block any other applications from being executed by using **Software Restriction Policies** or **AppLocker**.			
	(4)		**Disable default Administrative Shares.**[*1]			
		a)	To prevent unauthorized access using Administrative Shares, disable default Administrative Shares when they are not needed.	**Mandatory**	-	
		b)	When it is impossible to disable the feature described in a), use OS firewalls or other means to restrict the IP addresses to be allowed to use Administrative Shares.	**Mandatory** (Limited)	-	

Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.

2.2 Mitigating Vulnerabilities (2/2)

No.		Security Measures	Requirement Level	Recommended Value	Remarks
4	(5)	**Prevent external media drives from running anything automatically.** To mitigate threats from autorun malware, disable the autoplay/autorun feature in order to prevent applications from being executed automatically when they are attached in a external media drive.	Recommended	Restrict any media/devices running something automatically.	
	(6)	**Install antivirus software on servers (Windows) used for sharing files in the organization.** When you have one or more file servers for your organization, install antivirus software on them to prevent malware infection and detect such infection in the early stage.	**Mandatory**	-	
	(7)	**Install GCAPS software in all the servers running Windows OS.** To mitigate risks of vulnerabilities in servers, install GCAPS software.	**Mandatory**	-	
	(8)	**Restrict the use of Task Scheduler.** Allow only certain accounts to use an AT Command to run Task Scheduler. (Restrict granting accounts with the Administrator privileges.)	**Mandatory (Limited)**	-	

Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.

2.3 Strengthening Network Security

Restrict access more strictly to prevent attacks over the network to the intranet.

No.			Security Measures	Requirement Level	Recommended Value	Remarks
5	(1)		**Limit the target scope of the service by restricting access to the server.**			
		a)	In the inbound communication, allow only necessary minimum traffic by using filtering feature of network equipment or OS firewalls.	**Mandatory**	-	
		b)	In the outbound communication, allow only necessary minimum traffic by using filtering feature of network equipment or OS firewalls.	**Mandatory (Limited)**	-	
	(2)		**Restrict access to the network from an anonymous user.**	**Mandatory**	See 3.3	
			Use appropriate **Security Options** and/or other security settings methods to prohibit anonymous users from obtaining information. ➢ Restrict anonymous enumeration of SAM accounts and shares. ➢ Restrict allowing anonymous SID/Name translation.			
	(3)		**Configure the network logon authentication to be strict.**	**Mandatory**	See 3.3	
			Use **Security Options** and/or other security settings to prevent unauthorized access from avoiding authentication. ➢ Enhance LAN Manager authentication level. ➢ Prevent LAN Manager from storing hash values.			

**Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.*

2.4 Strengthening Operation Security (1/2)

Operational enhancement for early detections of attacks and/or indicators

No.			Security Measures	Requirement Level	Recommended Value	Remarks
6	(1)		**Obtain information on security issues of servers you are using from the Security Control Center, vendors and other appropriate sources, check the details and fix vulnerabilities if there is any.**	**Mandatory**	-	
			Use VPS and other appropriate sources to obtain vulnerability information about OSs, applications, hardware and any resources on your servers. Build a plan to install security patches and implement them. If no security patch is provided, consider the alternative to mitigate the vulnerability.			
	(2)		**Collect logs required to detect the sign of an incident and respond to it properly.**			
		a)	When you are providing services using one or more Web servers, ftp servers, PROXY servers, mail servers or any other similar servers, reserve both sending and receiving log records of such services.*	**Mandatory**	-	
		b)	Configure **Security Audit Policy** to collect authentication logs.	**Mandatory**	See 3.4	
		c)	Collect network access logs by using network equipment and/or OS firewall functions.	**Mandatory (Limited)**		
		b)	Collected logs must be retained for a certain period of time.	**Mandatory**	One year or more	

**Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.*

2.4 Strengthening Operation Security (2/2)

No.			Security Measures	Requirement Level	Recommended Value	Remarks
6	(3)		**Monitor logs regularly.**			
		a)	To limit the damage caused by ID spoofing and similar threats to the minimum at the early stage, monitor authentication logs on a regular basis.	**Mandatory (Limited)**	Monthly check	
		b)	To detect signs of unauthorized access, monitor traffic sources attempting to access locations other than service ports by analyzing firewall logs and other records on a regular basis.	**Mandatory (Limited)**	Monthly check	
	(4)		**Check regularly what programs run at startup.**	**Mandatory**	Check in every three months	Before actually using **Autoruns**, you must validate that there is no problem in running it.
			When a server gets infected with malware, the settings tend to be manipulated to have it run a malicious program. Use **Autoruns** or a similar tool on a regular basis confirm that there is not any settings to allow unauthorized file to be executed at startup.			
	(5)		**Accounts of administrators/operators must be strictly managed and operated.**			
		a)	Check all the account on a regular basis to delete/lock unnecessary accounts.	**Mandatory**	Check in every three months	
		b)	Do not use a common account.	**Mandatory**	-	
		c)	Do not logon with Administrator privileges.	Recommended	-	
		d)	Do not use the same password as used for other systems.	**Mandatory**	-	Note that this rule does not apply to NEC Group Authentication User ID and Password.

**Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.*

2.5 Strengthening Operation Terminal Security (1 / 2)

Prevent operation terminals from being used as a starting point by attackers attempting to steal credentials.

No.		Security Measures	Requirement Level	Recommended Value	Remarks
7	(1)	**Operation terminals must be dedicated to operation.** Because a business PC is used for handling e-mails and web content, they are exposed to high risk of malware infection. Operation terminals must be dedicated to operation.	Mandatory (Limited)	-	
	(2)	**Restrict the use of Task Scheduler.** Allow only certain accounts to use an AT Command to run Task Scheduler. (Restrict granting accounts with the Administrator privileges.)	Mandatory (Limited)	-	
	(3)	**Avoid using Active Directory when it is possible.** When you have to use an Active Directory, additional security measures to maintain the required security level is necessary.	Mandatory (Limited)	-	When you have to use an Active Directory, use the NEC Group ZENSYA Windows Domain System.
	(4)	**Do not use a password that was used for other terminals/servers.** Using a shared password makes intrusion to the system more easy; use a unique password for a terminal or a server.	Mandatory (Limited)	-	
	(5)	**Disable default Administrative Shares.** a) To prevent unauthorized access using Administrative Shares, disable default Administrative Shares when they are not needed. b) When it is impossible to disable the feature described in a), use OS firewalls or other means to restrict the IP addresses to be allowed to use Administrative Shares.	Mandatory (Limited)	-	

Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.

2.5 Strengthening Operation Terminal Security (2 / 2)

Prevent attacks on servers by removing authentication data.

No.		Security Measures	Requirement Level	Recommended Value	Remarks
7	(6)	**Limit the target scope of the service by restricting access to the server.**	**Mandatory (Limited)**	–	
		In the inbound communication, allow only necessary minimum traffic by using filtering feature of network equipment or OS firewalls.			
		In the outbound communication, allow only necessary minimum traffic by using filtering feature of network equipment or OS firewalls.			

Note that values recommended in reference guides are not mandatory; use them to broaden your perspective.

3. Reference

3.1 Strengthening Password Policy

Place to set up

- To set up Password Policy, go to:
  Start -> **Administrative Tools** -> **Local Security Policy** -> **Account Policies** -> **Password Policy**
- To set up Security Options, go to:
  Start -> **Administrative Tools** -> **Local Security Policy** -> **Local Policies** -> **Security Options**

Recommended values for configuration

For configuration, MIS Tokyo recommends to adopt values shown in the table below unless you have any specific reason such as they may affect your services/operations.

No	Security Measures	Recommended value	Remarks
1	**Password Policy**		
	Minimum password length Define the minimum required length for a password.	8 letters or more	
	Minimum password life Define the period during which changing a password is prohibited in order to prevent the password from being reused in a short period of time.	One day or more	
	Maximum password life To limit the possible abusive in case credentials leaks, an effective period for a password must be defined.	90 days or less	
	Enforce password history. Set up to record the change history of reserved passwords to prevent a single password from being used for another system.	11 records or more	
	Password must meet complexity requirements To prevent a vulnerable password from being created, a password must contain at least three of the following four types of characters: capital letters (alphabet), small letters (alphabet), numbers and special characters.	Enabled	
	Store passwords using reversible encryption To reduce risks of password leaks, passwords must NOT be stored using reversible encryption.	Disabled	
	Security Options		
	Accounts: Limit local account use of blank passwords to console logon only Use of local accounts that are not protected by a password must be restricted only for console login.	Enabled	

* In reality, only passwords with 8 or more characters are allowed in accordance with other settings.

3.2 Strengthening Account Lockout Policy

Place to set up

- To set up the Account Lockout Policy, go to:
  Start -> **Administrative Tools** -> **Local Security Policy** -> **Account Policies** -> **Account Lockout Policy**

Recommended values for configuration

For configuration, MIS Tokyo recommends to adopt values shown in the table below unless you have any specific reason such as they may affect your services/operations.

No.		Security Measures	Recommended value	Remarks
2	(1)	**Account lockout threshold** To mitigate risks of systematic brute-force attacks, set up this policy to determine the number of failed authentication attempts that will cause the account to be locked.	10 attempts or less	
	(2)	**Reset account lockout counter after** Designate the number of minutes for the period before the failed logon attempt counter is reset to 0 after the actual failed logon attempt. Enter the value smaller than the one set for the lockout duration.	15 minutes or more	
	(3)	**Account lockout duration** To mitigate risks of systematic brute-force attacks, designate the number of minutes for a certain period of time during which a locked-out account will not be authenticated.	15 minutes or more	

3.3 Strengthening Security Options

Place to set up

Start -> Administrative Tools -> Local Security Policy -> Local Policies -> Security Options

Recommended values for configuration

For configuration, MIS Tokyo recommends to adopt values shown in the table below unless you have any specific reason such as they may affect your services/operations.

No.		Security Measures	Recommended value	Remarks
3	(1)	**Accounts: Administrator account status** Disable the built-in Administrator account if it does not impose any impact on your system (for example, when there is no application using the built-in Administrator account).	Disabled	Select either (1) or (2) to implement this security measure.
	(2)	**Accounts: Rename administrator account** The built-in Administrator account cannot be deleted, but you can rename it name when it does not affect your system.	Rename the built-in administrator account to the one that will not remind any administrator privileges.	
5	(2)	**Network access: Do not allow anonymous enumeration of SAM accounts and shares** Do not allow anonymous users to list up Security Accounts Manager (SAM) accounts and network shares.	Enabled	
		Network access: Allow anonymous SID/Name translation Prohibit anonymous users from obtaining the real name of another user by using the security identifier (SID).	Disabled	For building a domain controller, you have to make this setting “Enabled”.
	(3)	**Network security: LAN Manager authentication level** Use secure protocol(s) for challenge/response authentication for network logons.	Send NTLMv2 responses only	
		Network security: Do not store LAN Manager hash value on next password change To prevent password leaks, prohibit LAN Manager hash value from being stored on a local computer when the password is changed.	Enabled	

3.4 Strengthening Event Log Audit

Place to set up

Start -> **Administrative Tools** -> **Local Security Policy** -> **Local Policies** -> **Audit Policy**

Recommended values for configuration

For configuration, MIS Tokyo recommends to adopt values shown in the table below unless you have any specific reason such as they may affect your services/operations .

No.	Security Measures	Recommended value	Remarks
6-(2)b)	**Audit account logon events** When a domain user account is authenticated by domain controller, it is recorded as an account logon event. You can set the auditing policy to audit Success, Failure, Success and Failure or No Auditing of logon events.	Success/ Failure	
	Audit account management Audit events such as creation, change, deletion of an user account and creation and change of a password.	Success/ Failure	
	Audit system events Audit when a user restarts or shuts down the computer; or an event has occurred that affects either the system security or the security log.	Success/ Failure	
	Audit policy change Audit every incidence of a change to security options, audit policies, user rights assignment, or trust policies.	Success/ Failure	
	Audit logon events Audit each instance of a user logging on, logging off, or making a network connection to the computer.	Success/ Failure	

*For audit policies other than those described above, the administrator of each server is responsible for determining values and configuring based on them.

Caution:
The size of log files defers depending on settings. See the reference guide shown in P11 of this document and set the properties such as **Maximum log size** and **When the maximum log size is reached** appropriately to enable log files to be reserved for one year or more.

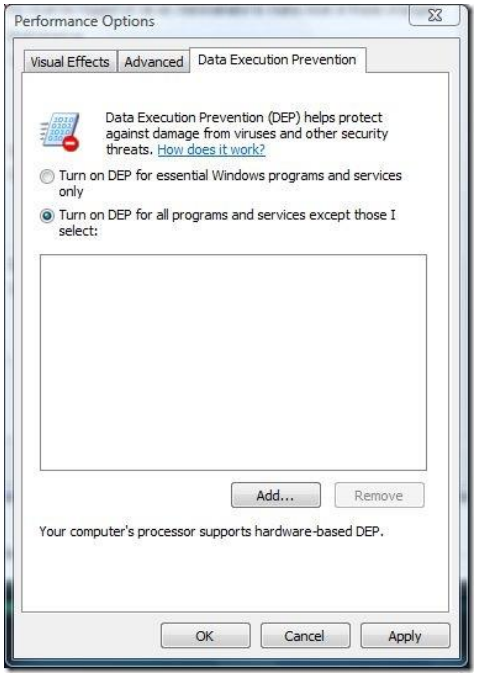
3.5 Enabling Data Execution Prevention (DEP)

Starting DEP

1. Click **Start**. Right click **Computer** and select **Properties**.
2. Select **Advanced system settings**.
3. When the System Properties window opens, select the **Advanced** tab and click **Settings...** of Performance.
4. When the Performance Options window opens, select the **Data Execution Prevention** tab.

Setting Up DEP

- Check DEP settings and confirm that the following sentence is marked.
  - **Turn on DEP for all programs and services except for those I select:**
- When you see the other sentence **Turn on DPE for essential Windows programs and services only** is marked, change the setting as described above. When the following occurs after the change, add the application as exception of DEP.
  - When you start an application, an error message is displayed and the application is automatically terminated.
  - When you try to start an application, it is not started and nothing appears.



The default setting of Windows Server 2003 SP1 and later is "Turn on DEP for all programs and services except for those I select:".

3.6 Using EMET (1/2)

What is the Enhanced Mitigation Experience Toolkit (EMET)?

- EMET is a free tool Microsoft provides to prevent malware from exploiting vulnerabilities by using security mitigation technologies such as:

- **Data Execution Prevention (DEP)**
  Prevents malware from being executed in the data segment. (Implemented in XP SP2 or later)
- **Structured Exception Handling Overwrite Protection (SEHOP)**
  Prevents attackers that exploit buffer overflow vulnerability. (A standard feature for VISTA SP1 or later)
- **Null-page pre-allocation (NullPage)**
  Blocks attacks that are going to take advantage of NULL dereferences.
- **Heap Spray address pre-allocation (HeapSpray)**
  Blocks Heap Spray attacks.
- **Bottom-Up virtual memory randomization (BottomUpASLR)**
  Blocks shellcodes from working by randomly allocating base addresses to secure memories such as heaps and stacks.
- **Export Address Table Access Filtering (EAF)**
  Prevents shellcodes from working by controlling reading and writing in the Export Address Table.
- **Address Space Layout Randomization (ASLR)**
  Blocks shell codes from working by randomly placing address spaces.

3.6 Using EMET (1/2)

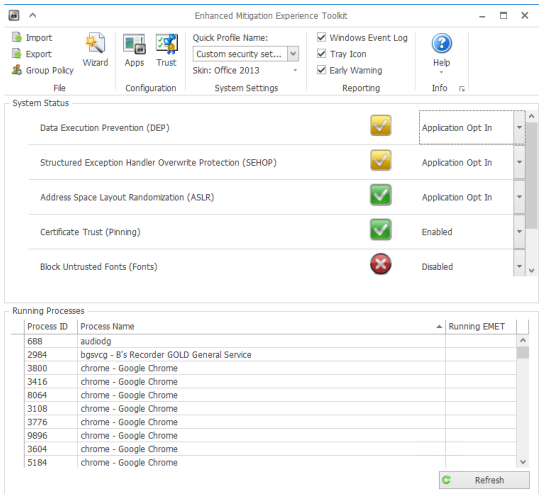
Installing EMET

1. Download the EMET Version 5.5 from the following website:
   https://www.microsoft.com/en-us/download/details.aspx?id=50766
2. Execute the downloaded **EMET Setup.msi** and install it.
   Select the installation folder and click **Everyone** for the target scope of EMET.
3. Follow the instructions for installation.

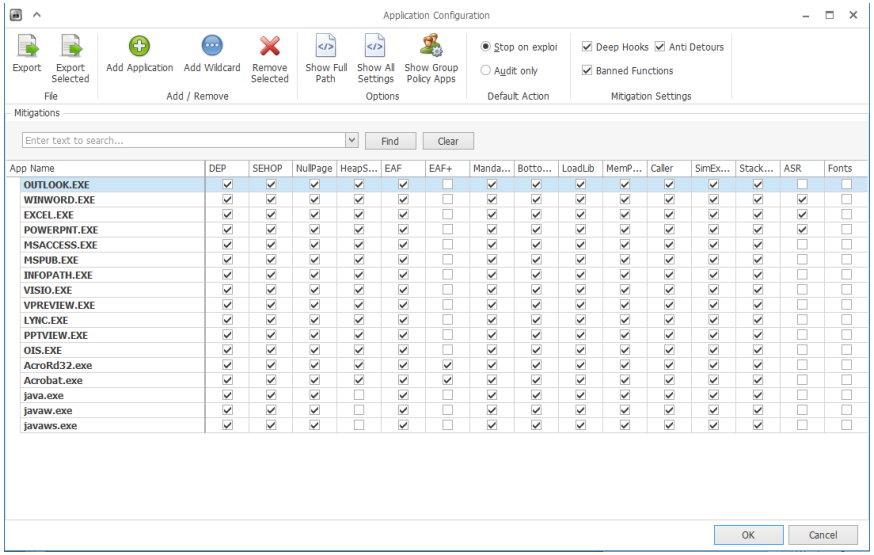
Using EMET

Below are steps for adding applications to be protected by EMET.

1. **Start** -> **All Programs** -> **Enhanced Mitigation Experience Toolkit**. Select **EMET 5.5** to start EMET.
2. Click **Apps**.
3. When **Application Configuration** starts, Click **Add Application**.
4. In the **Add Application** window, select application(s) to be protected by EMET.
5. In the **Application Configuration**, mark the feature(s) you want to use and click **OK**. You have to restart the machine to use **EMET**.



3.6 Using EMET (2/2)



➢ Using default profiles

You can use EMET default profiles to determine applications to be protected.

1) Start **Application Configuration**. (See the previous page “Using EMET” 1-2 for the starting flow.)
2) From the **File** menu, select **Import…**. In **Import Settings**, select **All.xml** in the directory ”C:¥Program Files¥EMET¥Deployment¥Protection Profiles”.

   *You can use the following profiles:

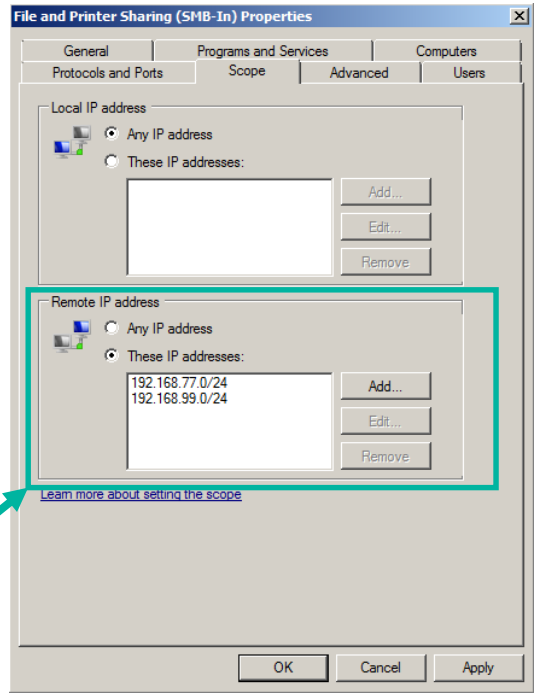
   - Internet Explorer.xml: Protects Internet Explorer only.
   - Office Software.xml: In addition to Internet Explorer, protects Microsoft Office and Adobe Reader/Acrobat.
   - All.xml: Protects general applications as well as those described above.
     (For details of the applications to be protected, please confirm the XML files.)

3) After confirming the imported settings, crick **OK** and restart your Windows.

3.7 Restriction on Administrative Shares by Filtering

The following example shows how to set up the scope of IP addressees to be allowed to access the administrative shares by using Windows Firewall with Advanced Security on Windows Server 2008.

- Designating IP addresses to be allowed for administrative shares
  1. Start Windows Firewall with Advanced Security.
     Go to **Start** -> **Administrative Tools** -> **Windows Firewall with Advanced Security**.
  2. Both for **Inbound Rules** and **Outbound Rules**, set the scope in every effective **File and Printer Sharing**.
  3. Designate IP addresses to allow access.
     Click the **Scope** tab of the **Properties** window of the Rules and write IP addresses to allow access in the **Remote IP address** field.



3.8 Points for monitoring logs

Critical Logs in Auditing to Block Targeted Attacks

Event Logs (Security Logs)

Check event logs closely, especially if they are for authentication, to confirm there is not any:

- Remote access from an unauthorized remote desktop

by analyzing information such as user name, logon type and workstation name.

Firewall Logs

By using Windows firewall, you can obtain logs containing information described in the right table.

Check the logs to confirm that:

- there is no access to the port 445, which is a port used for access to an administrative share, from an IP address that is not allowed to access any admin share.
- there is access attempts from a single IP address to ports that are not in service one after another.

Data	Description
date, time	Date and time of a connection
action	OPEN, CLOSE (for opening and closing a connection respectively) DROP (for dropping a connection) INFO-EVENTS-LOST (for events processed but not recorded)
protocol	Protocol used (eg. TCP, UDP, ICMP)
src-ip, dst-ip	Source IP address, destination IP address
src-port, dst-port	Source port number, destination port number
size	Packet data size
tcpflags	TCP Control flags (S: Syn, A: Ack, F: Fin, R: Reset, etc.)
tcpsyn, tcpack	TCP sequence number in the packet
tcpwin	TCP window size in the packet
icmptype, icmpcode	Type and code of ICMP, respectively
info	Complementary information

3.9 Using Autoruns

What is Autorun?

- Autoruns shows a list of programs that run automatically when the PC starts. You can switch on/off of the automatic start feature of each entry.
- It is a free tool provided by Microsoft that requires no installation processes.

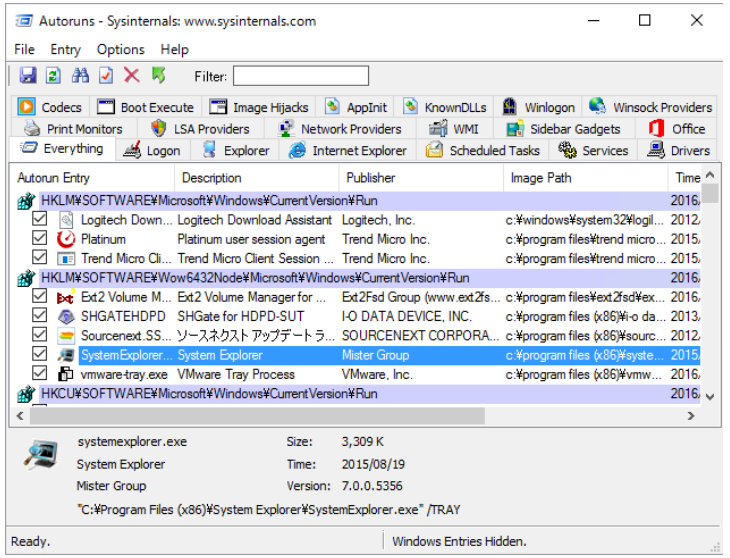
How to Use Autoruns

1. Download “Autoruns.zip” from “Download Autoruns and Autorunsc” at:
   https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
2. Unfold Autoruns.zip and execute “autoruns.exe” using the administrator privilege.

Points to be checked

When a screen that looks like the right image appears, check the following:

- Compare it with the previous application list to confirm that a strange application has not been added.
  - Save entry information by clicking **Save…** from the **Fine** menu and manage the entry history.
  - To compare the values of current entry information with information of the past, use **Compare…** of the **File** menu and open the file you want to compare (files with the extension “.arm“). The difference is shown in green.
- Confirm that there is no program whose Publisher field is blank.
  - Unlike general software, malware often does not have a publisher name.
  - Go to **Options** -> **Filter Options** and turn on **Verify code signature**, and you can validate digital signatures



Caution:
When you are using the VirusScan antivirus software, the VirusScan icon in the task tray may be surrounded by red lines depending on the applied access control rules. This does not indicate any problems and you can ignore the red line.


Orchestrating a brighter world
NEC