

LAB 2.1. NGĂN CHĂN DÙNG PHẦN MỀM TRÊN WINDOWS 7

I. GIỚI THIỆU

Bài lab dùng 01 máy Windows 7 thực hiện các thao tác cấu hình ngăn chặn người dùng sử dụng một số phần mềm.

Các bước thực hiện:

A. Chuẩn bị

- 1. Kích hoạt user account built-in Administrator & cài Yahoo Messenger
- 2. Tạo 2 user account dùng chương trình Yahoo Messenger

B. Dùng Software Restriction Policies cấm user dùng chương trình Calculator - Kiểm nghiệm

C. Dùng Application Locker cấm user dùng Yahoo Messenger

- 1. Kích hoạt dịch vụ Application Identity
- 2. Cấu hình ApplicationLocker Kiểm nghiệm



II. THỰC HIỆN

- A. Chuẩn bị:
- 1. Kích hoạt user account built-in Administrator & cài Yahoo Messenger
- Start \rightarrow Click phải Computer \rightarrow Chọn Manage







- Bo chon muc Account is disabled \rightarrow Apply \rightarrow OK



- Log off

- Log on administrator. Cài Yahoo Messenger



GOLD CERTIFIED

Partner

2. Tạo 2 user account

- Start \rightarrow Click phải Computer \rightarrow Chọn Manage

- Computer Management \rightarrow System Tools \rightarrow Local Users and Groups \rightarrow Users \rightarrow Click phải Users \rightarrow chọn New Users

| 🛃 Computer Manageme | ent | | | |
|---|--|--|--------------------------------|---|
| File Action View Image: Second secon | Help 🗟 🛛 🔀 | Þ | | |
| 🛃 Computer Managem | ient (Local | Name | Full Name | Description |
| W System Tools Task Schedule Event Viewer Shared Folder Local Users ar Userr Grou N Perform Device N Storage Disk Ma Services and | er nd Groups New User View Refresh Export Lis Help | Administr Guest HomeGro NhatNgh | ator up HomeGroupUser! e | Built-in accour Built-in accour S Built-in accour |

- Ở mục User name, đặt tên u1. Ở mục Password và Confirm Password, nhập 123 → Create

| New User | | | ? X |
|------------------|-----------------------|--------|-------|
| User name: | u1 | | |
| Full name: | | | |
| Description: | | | |
| | | | |
| Password: | ••• | | |
| Confirm password | l: ••• | | |
| User must cha | ange password at next | logon | |
| User cannot o | hange password | | |
| Password nev | ver expires | | |
| Account is dis | abled | | |
| | | | |
| | | | |
| Help | | Create | Close |





- Tương tự tạo thêm user u2, password: 123

| 🚇 Computer Management | | | |
|--|-----------------|-----------------|-------------------------------------|
| File Action View Help Image: Contract of the second | | | |
| 🜆 Computer Management (Lc 🔺 | Name | Full Name | Description |
| ▲ [™] | 🜆 Administrator | | Built-in account for administering |
| Iask Scheduler | 👧 Guest | | Built-in account for guest access t |
| Event Viewer | 💭 HomeGroup | HomeGroupUser\$ | Built-in account for homegroup a |
| Shared Folders | 💭 NhatNghe | | |
| Eccal Users and Grou | 💭 u1 | u1 | |
| Groups | 🐙 u2 | u2 | |
| No Performance | | | |

- Log on ul \rightarrow sign in Yahoo Messenger \rightarrow Thành công.
- Log on u2 \rightarrow sign in Yahoo Messenger \rightarrow Thành công.



16. COM/H



B. Dùng Software Restriction Policies cấm user dùng chương trình Calculator

- Start \rightarrow khung Search programs and files \rightarrow nhập **Calculator**



- Kiểm tra thấy chương trình Calculator hoạt động tốt

| Calculator | | | | | | | | |
|------------|---|--------|------|----|-----|--|--|--|
| View | E | idit H | lelp | | | | | |
| | 0 | | | | | | | |
| м | c | MR | MS | M+ | M- | | | |
| - | - | CE | С | ± | √ | | | |
| 7 | | 8 | 9 | / | % | | | |
| 4 | • | 5 | 6 | * | 1/x | | | |
| 1 | | 2 | 3 | - | | | | |
| | | | | | | | | |
| | _ | - | | | | | | |



- Start \rightarrow khung Search programs and files \rightarrow nhập **gpedit.msc**.

| Programs (1) | | |
|--------------------------|---|------------|
| 📕 gpedit | | |
| | | |
| | | |
| | (a) the second se | |
| | and the second second | |
| | - | |
| | | D |
| | | 2 |
| | | |
| | | |
| | | |
| | | 5 |
| ₽ See more results | | Q |
| gpedit.msc × Shut down + | | O |
| | | <u>a</u> 5 |
| 🤭 🌽 🔚 🔍 🖳 | | e |

- Computer Configuration \rightarrow Windows Settings \rightarrow Security Settings \rightarrow Software Restriction Policies \rightarrow click phải \rightarrow New Software Restriction Policies.

| Local Group Policy Editor | | |
|---|-------------------|--|
| File Action View Help | | |
| 🗢 🔿 🞽 📰 🔽 🖬 | | 2 |
| Local Computer Policy | | 2 |
| Computer Configuration | | No Software Restriction Policies Defined |
| Software Settings | | - |
| Windows Settings | | Software restriction policies are not defined in this Group Policy |
| Name Resolution Policy | | object. If you define software restriction policies in this Group |
| Scripts (Startup/Shutdown) | | Policy object, they will override inherited policy settings from |
| Deployed Printers | | other Group Policy objects. |
| Security Settings | | To define software restriction policies, in the Action menu, click |
| Account Policies | | New Software Restriction Policies. |
| Local Policies | 10 | |
| Windows Firewall with Advar Network List Message Delisit | nced Security | Note: After initially creating software restriction policies, a |
| Network List Manager Policie Dublic Key Deliging | 25 | reboot is required before they will be enforced. |
| Public Key Policies | 1 | |
| Software Restriction Policies | New Software Part | vistion Deligion |
| Application Control Pol | New Software Kest | Inction Policies |
| Advanced Audit Policy | All Tasks | • |
| Policy-based QoS Administrative Templates | View | • |
| a 😢 User Configuration | Help | |
| Software Settings | | |
| Windows Settings | | |
| Administrative Templates | | |
| Creates software restriction policies for this Grou | up Policy object. | , |
| ereates sector restriction policies for this offer | ip i oney objecti | |





GOLD CERTIFIED

Partner

- Click phải Additional Rules \rightarrow New Hash Rule.

| File Action View Help Image: Computer Policy Image: Computer Policy Image: Computer Policy Image: Computer Policy Image: Computer Policy Image: Computer Policy Image: Policy Image: Policy Image: Policy Image: Computer Policy Image: Policy Image: Policy Image: Policy Image: Policy Image: Policy Scripts (Startup/Shutdown) Image: Policy Image: Policy Image: Policy Image: Policy Scripts (Startup/Shutdown) Image: Policy Image: Policy Image: Policy Image: Policy Scripts (Startup/Shutdown) Image: Policy Image: Policy Image: Policy Image: Policy Scripts (Startup/Shutdown) Image: Policy Image: Policy Image: Policy Image: Policy Scripts (Startup/Shutdown) Image: Policy Image: Policy Image: Policy Image: Policy Mathinstative Terms Image: Policy Image: Policy Image: Policy Image: Policy Scripts Policy Image: Policy Image: Policy Image: Policy Image: Policy Policy Policy Image: Policy Image: Policy Image: Policy | Local Group Policy Editor | | | | l | - 🗆 X |
|--|---|--|------|----------------------|--|-------------|
| Image: Security Level Description Image: Security Settings Security Settings Image: Security Settings Security Levels Image: Security Settings Security Levels Image: Settings Security Levels | File Action View Help | | | | | |
| I Local Computer Policy Name Type Security Level Description Image: Software Settings ShtKEY_LOCAL_MACHINE\SOFTWARE\ Path Unrestricted Image: Software Settings ShtKEY_LOCAL_MACHINE\SOFTWARE\ Path Unrestricted Image: Software Settings ShtKEY_LOCAL_MACHINE\SOFTWARE\ Path Unrestricted Image: Software Settings Software Settings Software Settings Software Settings Image: Software Settings Software Settings Software Settings Software Settings Image: Software Settings Software Settings Name Software Settings Image: Software Settings Name Name Software Settings Image: Software Settings New Certificate Rule New Hash Rule Image: Software Settings New Path Rule New Path Rule Image: Software Settings New Path Rule New Path Rule Image: Software Settings New Path Rule New Path Rule Image: Software Settings New Path Rule New Path Rule Image: Software Settings New Path Rule New Path Rule Image: Software Settings New Path Rule | 🗢 🔿 🖄 🗊 📋 🗟 | 7 | | | | |
| | Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution I Scripts (Startup/Sh Deployed Printers Security Settings Account Polici Coal Policies Windows Firew Network List M Public Key Poli Software Restri Security Le Additi Additi Additi Advanced Policy-based Software Settings Software Settings Windows Settings Administrative Te Administrative Te | Policy nutdown) ies vall with Advanced Security Anager Policies icies iction Policies vels New Certificate Rule New Hash Rule New Network Zone Rule New Path Rule New Path Rule All Tasks View Refresh Export List Help | Name | Type Path Path | Security Level Unrestricted Unrestricted | Description |

- Browse.

| w Hash | Rule | | | | | | Σ |
|-----------|---------------------------------|--|---|-----------------------|--------------------------|-------------------------|-------------------|
| General | | | | | | | |
| 4010 | Use rul | es to overrid | le the def | ault sec | urity level | | |
| Giù | Click B attribute are aut | rowse to sel es, such as i omatically po | ect the fil its size an opulated. | e you wa id the da | ant to has ate and ti | sh. The fi me it was | ile's created, |
| | | | | | | E | Prowse |
| File info | mation: | | | | | | |
| | | | | | | | * |
| | | | | | | | |
| | | | | | | | Ŧ |
| Security | level: | Disallowe | d | | | | - |
| Descript | tion: | | | | | | |
| | | | | | | | * |
| | | | | | | | |
| | oro about | t software re | striction p | olicies | | | |
| Leam m | | | | | | | |



Partner

- Theo đến đường dẫn C:\Windows\System32 → Khung File name, nhập calc.exe → Open

| Organize 🔻 Nev | folder | | | |
|-----------------------------|--------|--------------------|----------------------|---|
| Desktop | ▲ N | ime | Date modified | Type |
| Downloads | _ | | | .,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| Recent Places | | 0409 | //14/2009 11:56 AM | Filefold |
| | | AdvancedInstallers | 7/14/2009 9:37 AM | File fold |
| 🚍 Librarier | | ar-SA | 7/14/2009 9:37 AM | File fold |
| | | bg-BG | 7/14/2009 9:37 AM | File fold |
| Music Pictures Videos | | Boot | 7/14/2009 11:56 AM | File fold |
| | | catroot | 7/14/2009 11:55 AM | File fold |
| | | catroot2 | 10/20/2009 1:45 AM | File fold |
| | | CodeIntegrity | 10/25/2009 4:23 AM | File fold |
| | | com | 7/14/2009 11:56 AM | File fold |
| Homegroup | | config | 10/20/2009 1:50 AM | File fold |
| | | cs-CZ | 7/14/2009 9:37 AM | File fold |
| Computer | | da-DK | 7/14/2009 9:37 AM | File fold |
| Local Disk (C:) | | de-DE | 7/14/2009 9:37 AM | File fold |
| 👊 Network | + 4 | Dirm | 7/14/2000 11:56 0.04 | Eile fald |
| | | | AU 51 (64) | |

- Bảo đảm chọn **Disallow**ed ở mục Security Level \rightarrow OK

| 1 | New Hash F | Rule | | 23 | | | | |
|---|-------------------------------------|--|--|-------------|--|--|--|--|
| | General | | | | | | | |
| | | Use rule Click Bro attribute are auto | is to override the default security level. owse to select the file you want to hash. The file's s, such as its size and the date and time it was creat matically populated. | ed, | | | | |
| | File infor | mation: | Browse | • | | | | |
| • | CALC.E CALC Window Microso | XE (6.1.70 vs Calculat ft® Windo | 600.16385) tor ws®Operating System | • • • | | | | |
| | Security | level: | Disallowed | • | | | | |
| | Descripti | ion: | | | | | | |
| | | | | * | | | | |
| | Learn mo | Learn more about software restriction policies | | | | | | |
| | | | OK Cancel Ap | oply | | | | |



GOLD CERTIFIED

Partner

- Kết quả

| 🗐 Local Group Policy Editor | | | |
|---|--|------------------------------|--|
| File Action View Help | | | |
| 🗢 🔿 🖄 🖬 📋 🖸 💀 🚺 | | | |
| Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Mindows Firewall with Advanced Security Network List Manager Policies Software Restriction Policies Software Audit Policies on Local Computer Advanced Audit Policy Configuration Policy-based QoS Administrative Templates Software Settings | Name %HKEY_LOCAL_MACHINE\SOFTWARE\ %HKEY_LOCAL_MACHINE\SOFTWARE\ CALC.EXE (6.1.7600.16385) CALC Windo | Type Path Path Hash | Security Level Unrestricted Disallowed |
| Windows Settings Administrative Templates | | | |
| | < III | | |
| | | | 2 |

- Khởi động lại máy → Log on user **Nhat Nghe**

- Start → khung Search programs and files → nhập Calculator → Chương trình Calculator không hoạt động được

| C:\Windo | ows\system32\calc.exe | |
|----------|---|----------|
| 8 | This program is blocked by group policy. For more information, contact your system administrator. | |
| | ОК | |
| | | iii 0 |





C. Dùng Application Locker cấm user dùng Yahoo Messenger

1. Kích hoạt dịch vụ Application Identity

- Log on administrator
- Start \rightarrow khung Search programs and files \rightarrow nhập Services.msc



- Nhấp kép service Application Identity
- Chọn kiểu khởi động: Automatic \rightarrow Apply \rightarrow chọn Start \rightarrow OK

| Application | n Identity | Properties (Local Computer) |
|---------------------|--------------------------|--|
| General | Log On | Recovery Dependencies |
| Service | name: | AppIDSvc |
| Display | name: | Application Identity |
| Descript | tion: | Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from |
| Path to C:\Wind | executable dows\syste | e: em32\svchost.exe -k LocalServiceAndNoImpersonation |
| Startup | type: | Automatic 👻 |
| Help me | e configure | e service startup options. |
| Service | status: | Stopped |
| S | itart | Stop Pause Resume |
| You car from her | n specify tł re. | he start parameters that apply when you start the service |
| Start pa | rameters: | |
| | | OK Cancel Apply |

Trang 11/18



Microsoft⁻

GOLD CERTIFIED

Partner

- Kết quả

| O, Services | | | |
|-------------------------------------|---|---------|----------------|
| File Action View Help | | | |
| ⇔ ⇒ 🔲 🖹 Q 🕞 🛛 🖬 🕨 🖛 | Þ | | |
| Services (Local) | | | |
| Application Identity | Name | Status | Startup Type |
| , appreciation rectartly | ActiveX Installer (AxInstSV) | | Manual |
| Stop the service | Adaptive Brightness | | Manual |
| Restart the service | Application Experience | Started | Manual |
| | 🕰 Application Identity | Started | Automatic |
| Description: | 🔍 Application Information | Started | Manual 🖉 |
| of an application. Disabling this | 🌼 Application Layer Gateway Service | | Manual |
| service will prevent AppLocker from | 🔍 Application Management | | Manual |
| being enforced. | 🌼 Background Intelligent Transfer Service | Started | Automatic (D 🚽 |
| | 🧠 Base Filtering Engine | Started | Automatic |
| | 🧠 BitLocker Drive Encryption Service | | Manual S |
| | 🤐 Block Level Backup Engine Service | | Manual S |
| | 🖾 Bluetooth Support Service | | Manual |
| Extended / Standard / | | | |
| | | | |

2. Cấu hình ApplicationLocker

- Start \rightarrow khung Search programs and files \rightarrow Nhập **GPEdit.msc**





Microsoft GOLD CERTIFIED Partner

- Computer configuration \rightarrow Windows settings \rightarrow Security settings \rightarrow Application control policies \rightarrow AppLocker \rightarrow Click phải Executable rules \rightarrow Create new rule.

| 🛒 Local Group Policy Editor | | | | |
|---|-------------|------|-------------------|-----------------------|
| File Action View Help | | | | |
| 🗢 🄿 🔽 📰 🗟 🖬 | | | | |
| Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Security Settings Local Policies Mindows Firewall with Advanced Security Settings Software Restriction Policies Software Restriction Policies Application Control Policies Applocker Script Rules Script Rules Signity Policy-based QoS Administrative Templates Windows Settings Software Settings | rity Action | User | Name There are | e no items to show ir |

- Next

| Create Executable Rules | | × |
|--|--|----|
| Before You Be | igin | |
| Before You Begin Permissions Conditions Publisher Exceptions Name | This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature. Before continuing, confirm that the following steps are complete: Install the applications you want to create the rules for on this computer. Back up your existing rules. Review the AppLocker documentation. To continue, click Next. Skip this page by default | |
| | < Previous Next > Create Cano | el |



GOLD CERTIFIED

Partner

- Chon Action **Deny** \rightarrow click Select

| Create Executable Rules | | × |
|--|---|-------|
| Permissions | | |
| Before You Begin Permissions Conditions Publisher | Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running. | |
| Exceptions Name | Action: ② Allow ③ Deny User or group: | |
| | Everyone Select | |
| | More about rule permissions | |
| | < Previous Next > Create C | ancel |

- Nhập $\mathbf{u2} \rightarrow \text{Check names} \rightarrow \text{OK}$

| Select User or Group | P | × |
|---|----------|-------|
| Select this object type: | | |
| User or Group | Object T | ypes |
| From this location: | | |
| PC11 | Locatio | ins |
| Enter the object name to select (examples): | | |
| PC11\u2 | Check N | lames |
| | | |
| | | |
| Advanced | OK Car | ncel |





Learning Solutions

- Next

| Create Executable Rules | X |
|--|---|
| Permissions | |
| Before You Begin Permissions Conditions Publisher | Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running. |
| Exceptions Name | Action: Allow Deny User or group: PC11\u2 Select |
| | More about rule permissions |
| | < Previous Next > Create Cancel |

- Bảo đảm dấu chọn ở mục **Publisher** → Next

| Create Executable Rules | × |
|--|---|
| Conditions | |
| Before You Begin Permissions Conditions Publisher Exceptions Name | Select the type of primary condition that you would like to create. Publisher Select this option if the application you want to create the rule for is signed by the software publisher. Path Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule. File hash Select this option if you want to create a rule for an application that is not signed. |
| | < Previous Next > Create Cancel |



GOLD CERTIFIED

Partner

Browse theo đường dẫn: "C:\Program Files\Yahoo!\Messenger" → chọn tập tin YahooMessenger → Open → Next

| Create Executable Rules Publisher | | | | 23 |
|--|--|---|---|----|
| Before You Begin Permissions Conditions Publisher Exceptions | Browse for a signed file to use as define the rule; as you move dov publisher position, the rule is ap Reference file: C:\Program Files\Yahoo!\Mess | s a reference for the rule. Use wn, the rule becomes more s plied to all signed files. enger\YahooMessenger.ex | the slider to select which properties pecific. When the slider is in the any Browse | |
| Name | Any publisher Publisher: Product name: File name: File version: Use custom values Rule scope: Applies to only the specified version | O=YAHOO! INC., L= YAHOO! MESSENGE 9.0.0.0 | SANTA CLARA, S=CA, C=US | |
| | | < Previous Nex | t > Create Cancel | |

- Next

| Create Executable Rules | | × |
|---|---|-------|
| Exceptions | | |
| Before You Begin Permissions Conditions Publisher <u>Exceptions</u> Name | Primary condition: "", in YAHOO! MESSENGER, from O=YAHOO! INC., L=SANTA CLARA, S=CA, C=US Add exception: Publisher | |
| | Exceptions: Exception Type Edit Remove | |
| | < Previous Next > Create Ca | incel |





Learning Solutions

- Create

| Create Executable Rules | X |
|--|---|
| Name and De | scription |
| Before You Begin Permissions Conditions Publisher | Enter a name to identify this rule. Name: "" in YAHOO! MESSENGER_from O=YAHOO! INC_L=SANTA CLARA_S=CA_C=US_ |
| Name | Description: (Optional) |
| | < Previous Next > Create Cancel |

- Hộp thoại AppLocker → Yes

| AppLocker | |
|-----------|--|
| A | The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system files will be allowed to run. Do you want to create the default rules now? |
| | Yes No |





- Kết quả

| Local Group Policy Editor | | | | | | | |
|---|-----|---|---|---|--|------------|--|
| File Action View Help | | | | | | | |
| | | | | | | | |
| Local Computer Policy Software Settings Windows Settings Software Settings Software Settings Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Windows Firewall with Advanced Security Network List Manager Policies Software Restriction Policies Software Restriction Policies Application Control Policies AppLocker Executable Rules Siript Rules | A H | Action S Deny Allow Allow Allow | User PC11\u2 Everyone EVeryone BUILTIN\Ad | Name "", in YAHOO! MESSENGER, from O=YA (Default Rule) All files located in the Pro (Default Rule) All files located in the Wi (Default Rule) All files | Condition Publisher Path Path Path | Exceptions | |
| Advanced Audit Policy Configuration | - | | | | | | |
| · · · · · · · · · · · · · · · · · · · | | | | | | | |

Log on u1 → sign in Yahoo Messenger → Thành công
 Log on u2 → sign in Yahoo Messenger → Thất bại.

| C:\Progr | am Files\Yahoo!\Messenger\YahooMessenger.exe | × | | | |
|---|--|----|--|--|--|
| This program is blocked by group policy. For more information, contact your system administrator. | | | | | |
| | | ОК | | | |