MODERN OPERATING SYSTEMS

LECTURE 10

AUTHOR: DR. ZVEREVA OLGA M.

AGENDA

- ➢ WINDOWS SECURITY SUBSYSTEM
  - ✓ SECURITY POLICY MANAGEMENT
  - ✓ LOCAL GROUP POLICY EDITOR
  - ✓ WINDOWS DEFENDER & WINDOWS DEFENDER SECURITY CENTER
  - ✓ UAC
  - ✓ EFS & BITLOCKER
- ➢ OS LINUX: USER INTERFACE

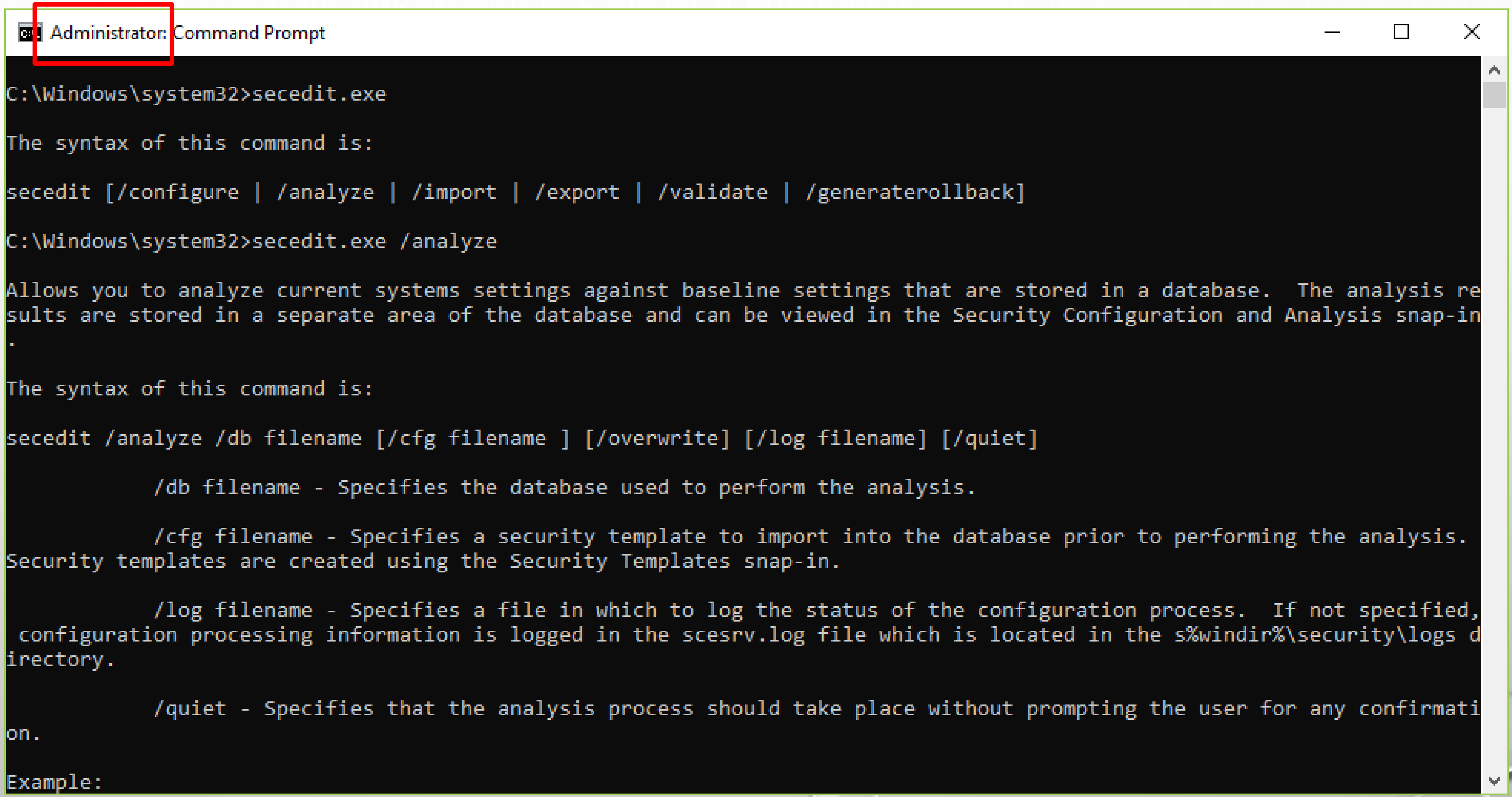
WINDOWS SECURITY SUBSYSTEM

1. SECURITY POLICY MANAGEMENT

SECURITY POLICY MANAGEMENT

- THERE ARE SEVERAL INSTRUMENTS TO CONFIGURE SECURITY POLICY:
  - ✓ **THE LOCAL SECURITY POLICY SNAP-IN** (SECPOL.MSC, CONTROL PANEL\ADMINISTRATIVE TOOLS\LOCAL SECURITY POLICY) - MMC SNAP-IN DESIGNED TO MANAGE ONLY SECURITY POLICY SETTINGS (SEE LECTURE 9)
  - ✓ **SECURITY EDITOR COMMAND LINE TOOL** (SECEDIT.EXE) - CONFIGURES AND ANALYZES SYSTEM SECURITY BY COMPARING YOUR CURRENT CONFIGURATION TO SPECIFIED SECURITY TEMPLATES
  - ✓ **SECURITY CONFIGURATION MANAGER TOOL –** THIS TOOL SET ALLOWS YOU TO CREATE, APPLY, AND EDIT THE SECURITY FOR YOUR LOCAL DEVICE, ORGANIZATIONAL UNIT, OR DOMAIN.
  - ✓ **GROUP POLICY** (GPEDIT.MSC) - THE GROUP POLICY MANAGEMENT CONSOLE USES THE GROUP POLICY OBJECT EDITOR TO EXPOSE THE LOCAL SECURITY OPTIONS, WHICH CAN THEN BE INCORPORATED INTO GROUP POLICY OBJECTS FOR DISTRIBUTION THROUGHOUT THE DOMAIN. THE LOCAL GROUP POLICY EDITOR PERFORMS SIMILAR FUNCTIONS ON THE LOCAL DEVICE.
  - ✓ **SECURITY COMPLIANCE MANAGER -** IS A DOWNLOADABLE TOOL THAT HELPS YOU PLAN, DEPLOY, OPERATE, AND MANAGE YOUR SECURITY BASELINES FOR WINDOWS CLIENT AND SERVER OPERATING SYSTEMS, AND FOR MICROSOFT APPLICATIONS

SECURITY EDITOR COMMAND LINE TOOL



```
C:\Windows\system32>secedit.exe

The syntax of this command is:

secedit [/configure | /analyze | /import | /export | /validate | /generaterollback]

C:\Windows\system32>secedit.exe /analyze

Allows you to analyze current systems settings against baseline settings that are stored in a database.  The analysis re
sults are stored in a separate area of the database and can be viewed in the Security Configuration and Analysis snap-in
.

The syntax of this command is:

secedit /analyze /db filename [/cfg filename ] [/overwrite] [/log filename] [/quiet]

            /db filename - Specifies the database used to perform the analysis.

            /cfg filename - Specifies a security template to import into the database prior to performing the analysis.
Security templates are created using the Security Templates snap-in.

            /log filename - Specifies a file in which to log the status of the configuration process.  If not specified,
 configuration processing information is logged in the scesrv.log file which is located in the s%windir%\security\logs d
irectory.

            /quiet - Specifies that the analysis process should take place without prompting the user for any confirmati
on.

Example:
```

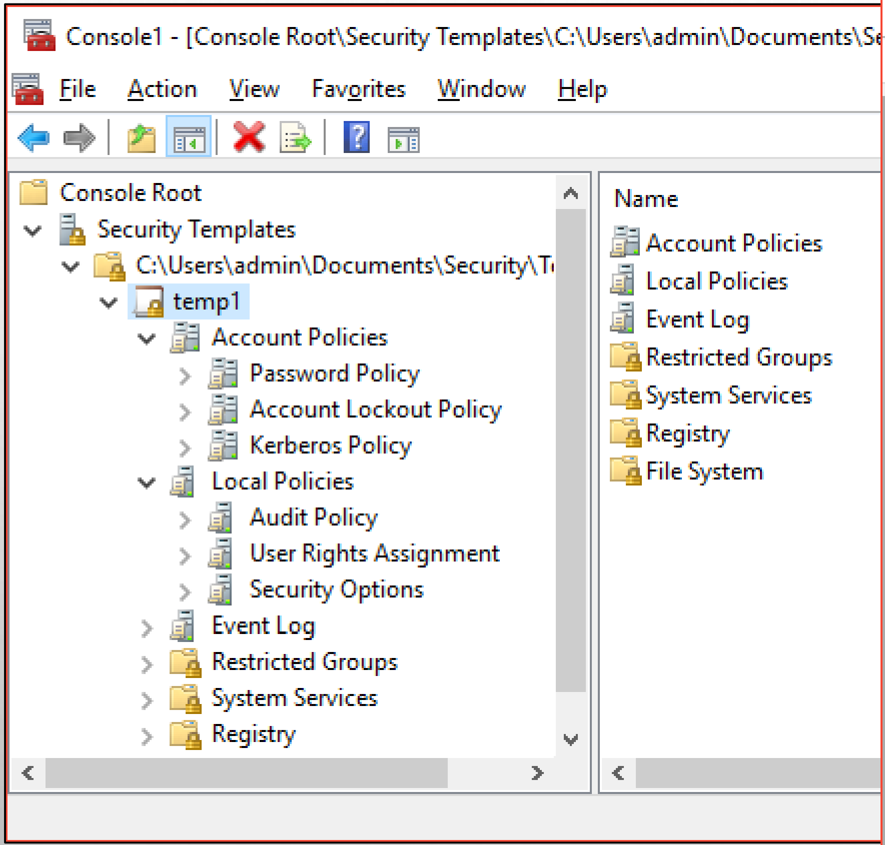
SECURITY CONFIGURATION MANAGER

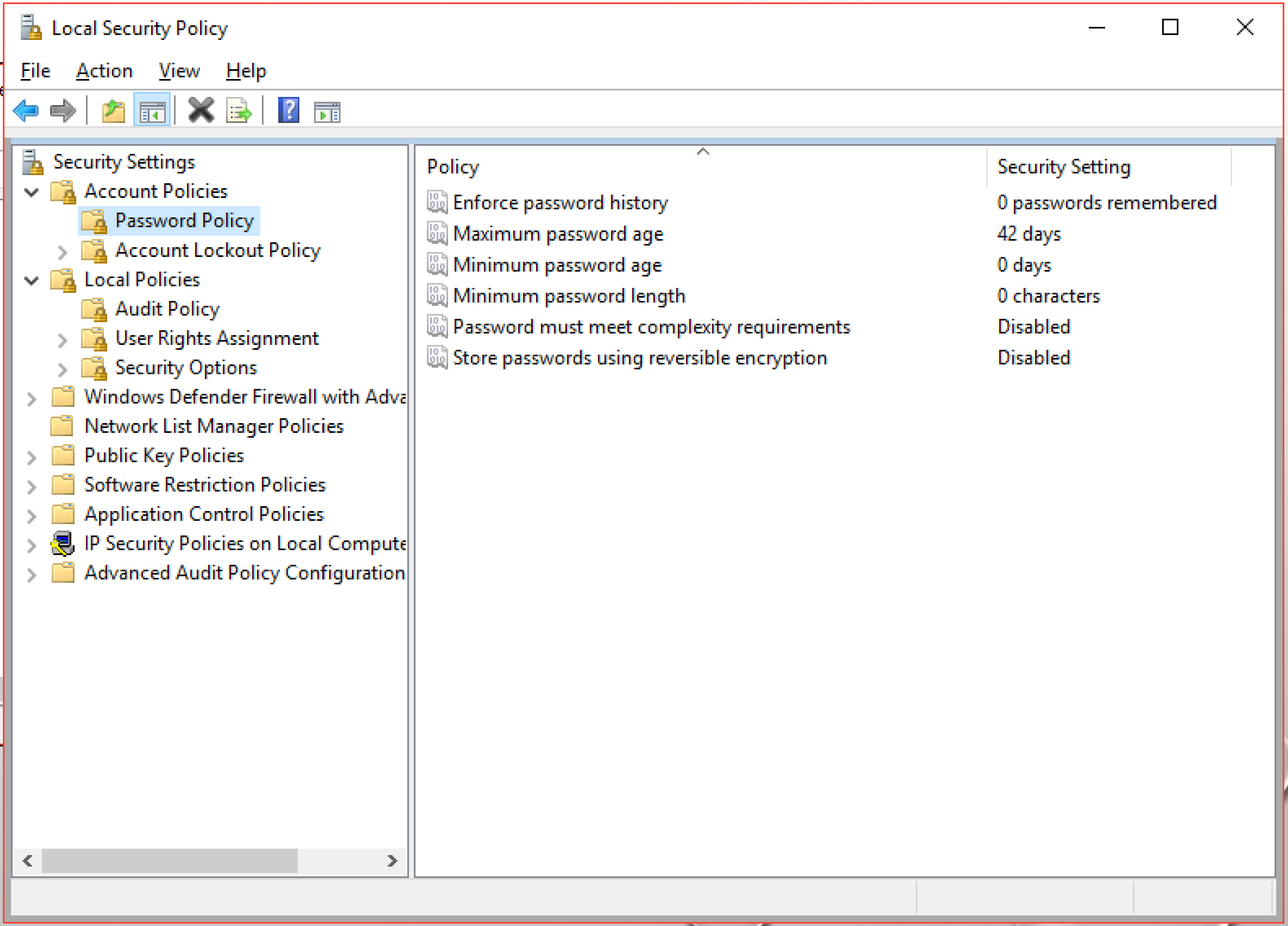
- ➢ ALLOWS YOU TO CREATE, APPLY, AND EDIT THE SECURITY FOR YOUR LOCAL DEVICE, ORGANIZATIONAL UNIT, OR DOMAIN.
- ➢ CONSISTS OF THE FOLLOWING TOOLS:
  - ✓ SECURITY TEMPLATES (DEFINES A SECURITY POLICY IN A TEMPLATE. THESE TEMPLATES CAN BE APPLIED TO GROUP POLICY OR TO YOUR LOCAL COMPUTER, OR USED FOR THE PURPOSE OF SECURITY ANALYSIS BY THE NEXT TOOL)
  - ✓ SECURITY CONFIGURATION AND ANALYSIS (DEFINES A SECURITY POLICY IN A TEMPLATE. THESE TEMPLATES CAN BE APPLIED TO GROUP POLICY OR TO YOUR LOCAL COMPUTER)
  - ✓ LOCAL SECURITY POLICY (HAS BEEN ALREADY DISCUSSED, SEE 46-54)

SECURITY TEMPLATES

- THIS SNAP-IN COULD BE INSTALLED IN MMC
- “THE SECURITY TEMPLATES” SNAP-IN DOES NOT INTRODUCE NEW SECURITY PARAMETERS, IT SIMPLY ORGANIZES ALL EXISTING SECURITY ATTRIBUTES INTO ONE PLACE TO EASE SECURITY ADMINISTRATION
- DEVELOPED TEMPLATES COULD BE **IMPLEMENTED,** OR USED **FOR COMPARIS**ON (ANALYSIS)
- A TEMPLATE IS SIMILAR (PARTIALLY) TO THE OBJECT OF THE “LOCAL SECURITY POLICY”
- TO APPLY A SECURITY TEMPLATE TO YOUR LOCAL DEVICE, YOU CAN USE “SECURITY CONFIGURATION AND ANALYSIS” SNAP-IN, OR THE SECEDIT COMMAND-LINE TOOL.

LOCAL SECURITY SETTINGS & SECURITY TEMPLATE

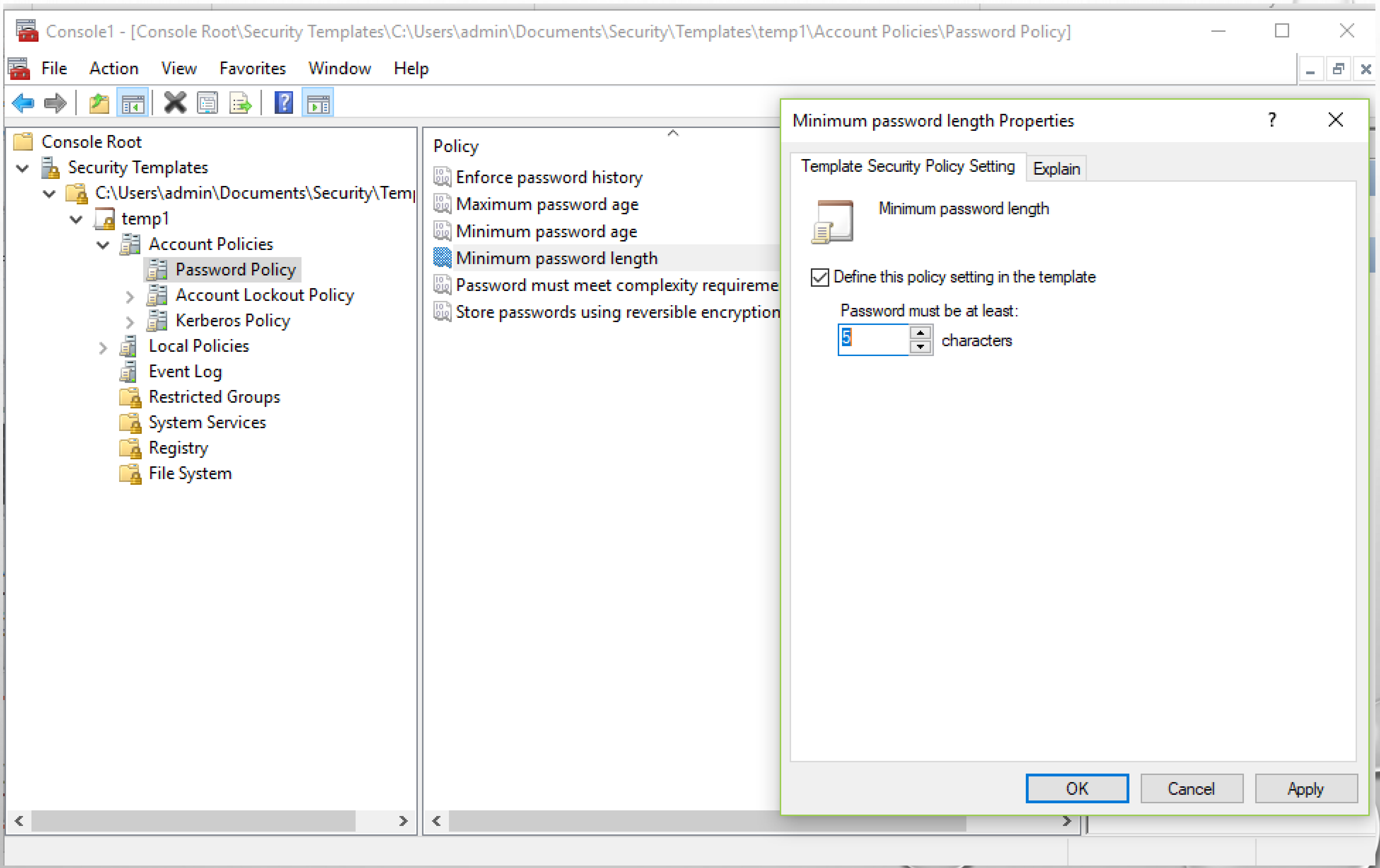




Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

CREATING NEW TEMPLATE



Console1 - [Console Root\Security Templates\C:\Users\admin\Documents\Security\Templates\temp1\Account Policies\Password Policy]

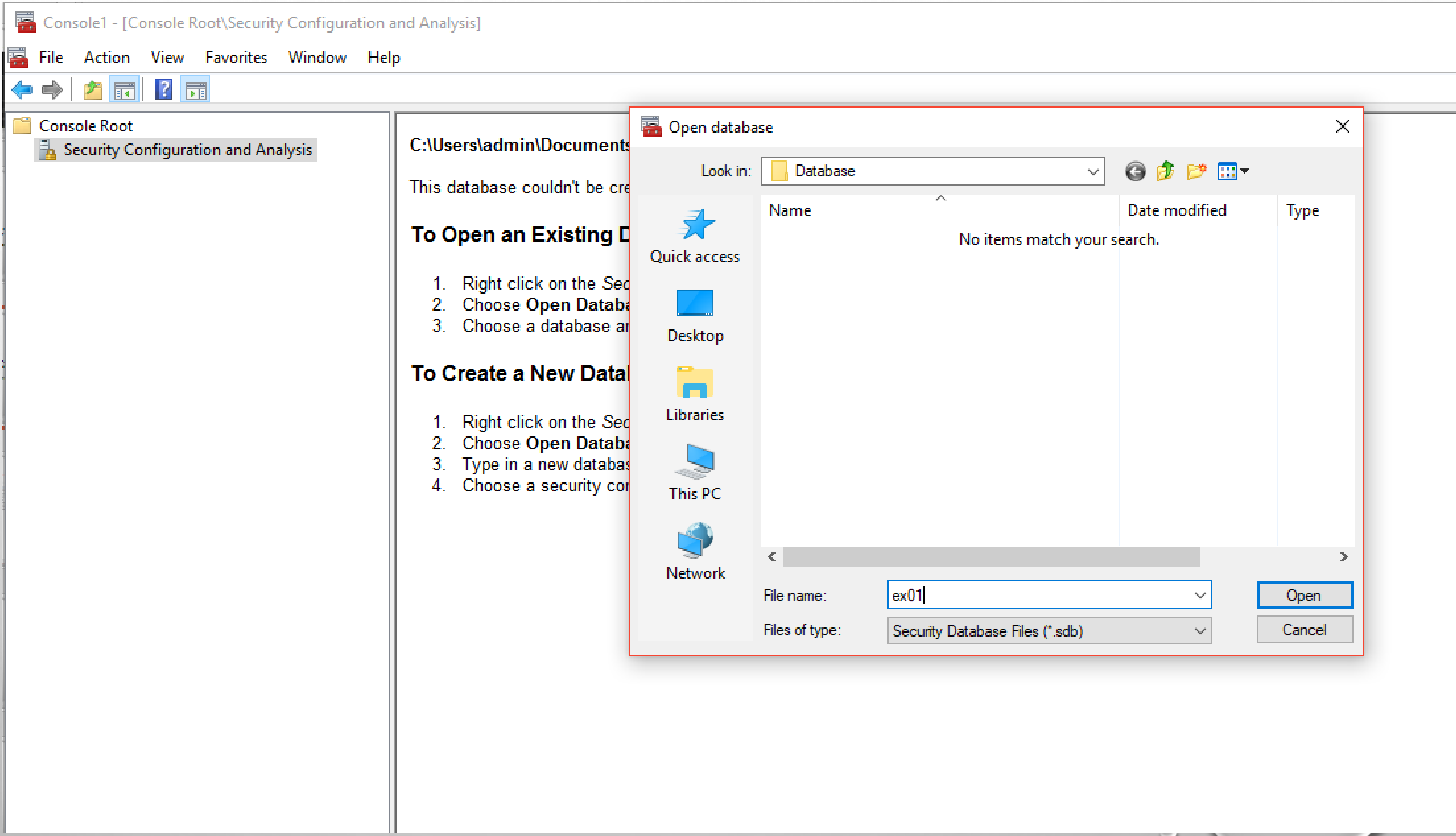
Minimum password length

☑ Define this policy setting in the template

Password must be at least:

5 characters

“SECURITY CONFIGURATION AND ANALYSIS” SNAP IN (1 STEP – CREATING NEW DATABASE)



C:\Users\admin\Documents

This database couldn't be cre

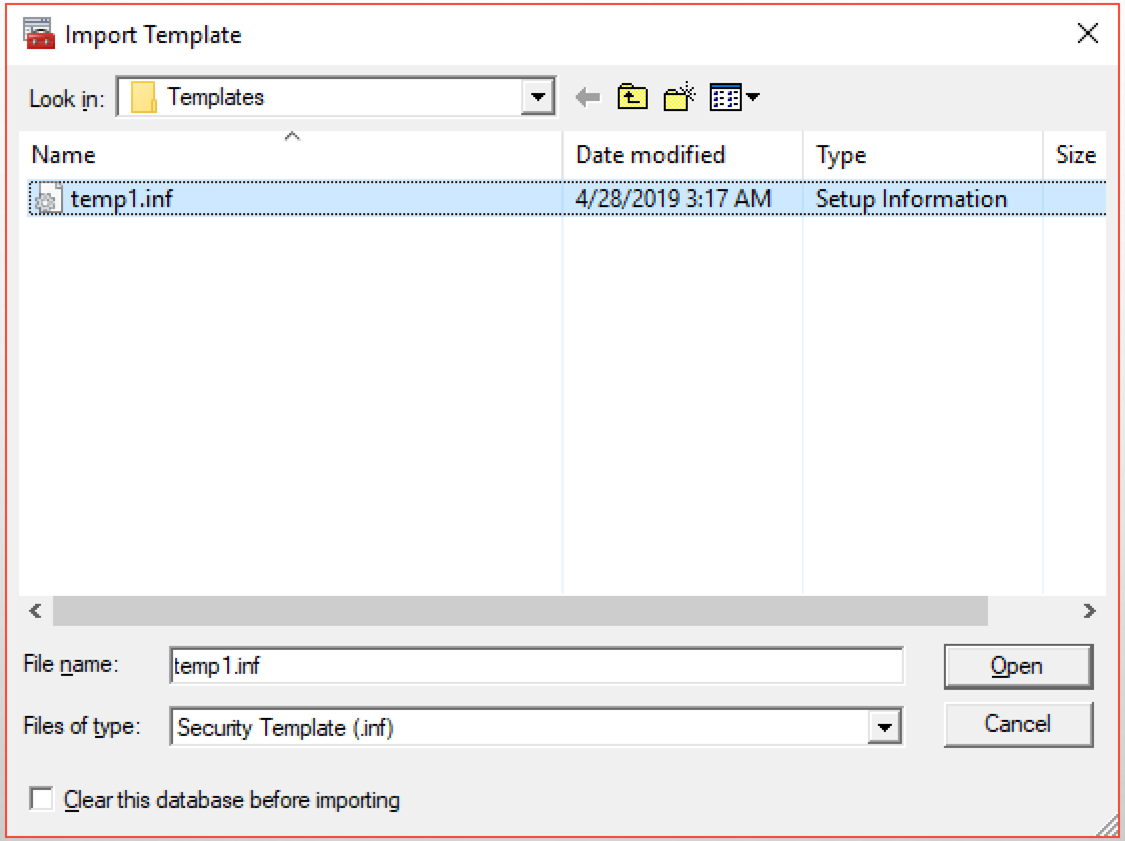
To Open an Existing D

1. Right click on the *Sec*
2. Choose **Open Databa**
3. Choose a database ar

To Create a New Datal

1. Right click on the *Sec*
2. Choose **Open Databa**
3. Type in a new databas
4. Choose a security cor

“SECURITY CONFIGURATION AND ANALYSIS” SNAP IN (2 STEP – IMPORTING THE PREDEFINED TEMPLATE INTO THE DATABASE)



Import Template

Look in: Templates

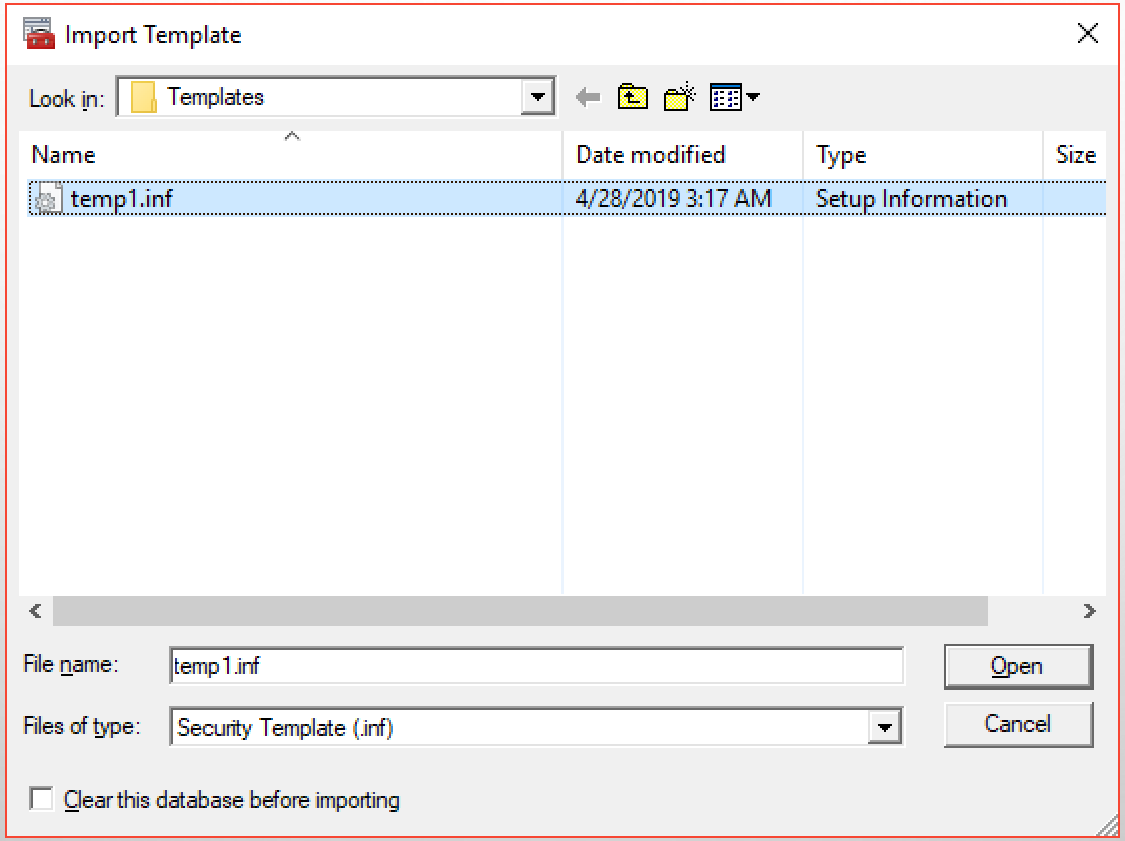
Name	Date modified	Type	Size
temp1.inf	4/28/2019 3:17 AM	Setup Information	

File name: temp1.inf

Files of type: Security Template (.inf)

□ Clear this database before importing

“SECURITY CONFIGURATION AND ANALYSIS” SNAP IN (3 STEP – IDENTIFYING ACTION: COMPARISON OR CONFIGURING COMPUTER)



Import Template

Look in: Templates

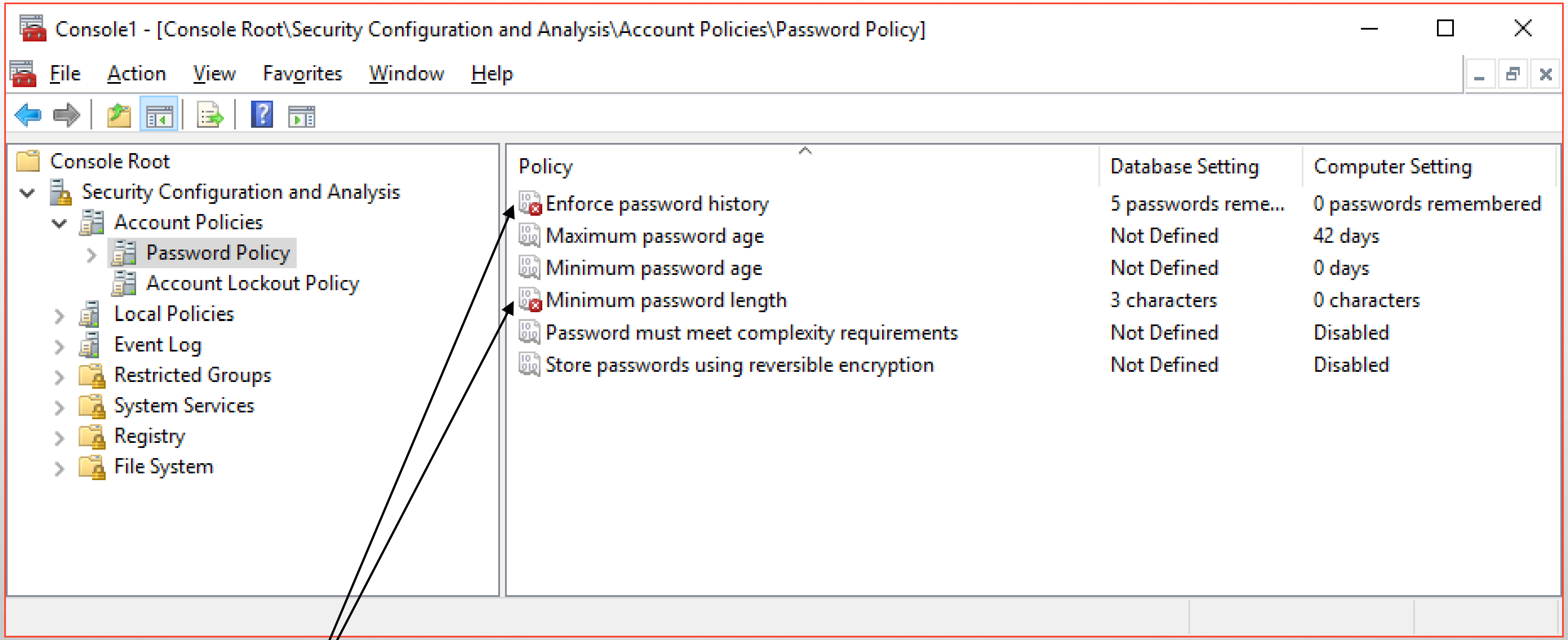
Name	Date modified	Type	Size
temp1.inf	4/28/2019 3:17 AM	Setup Information	

File name: temp1.inf

Files of type: Security Template (.inf)

□ Clear this database before importing

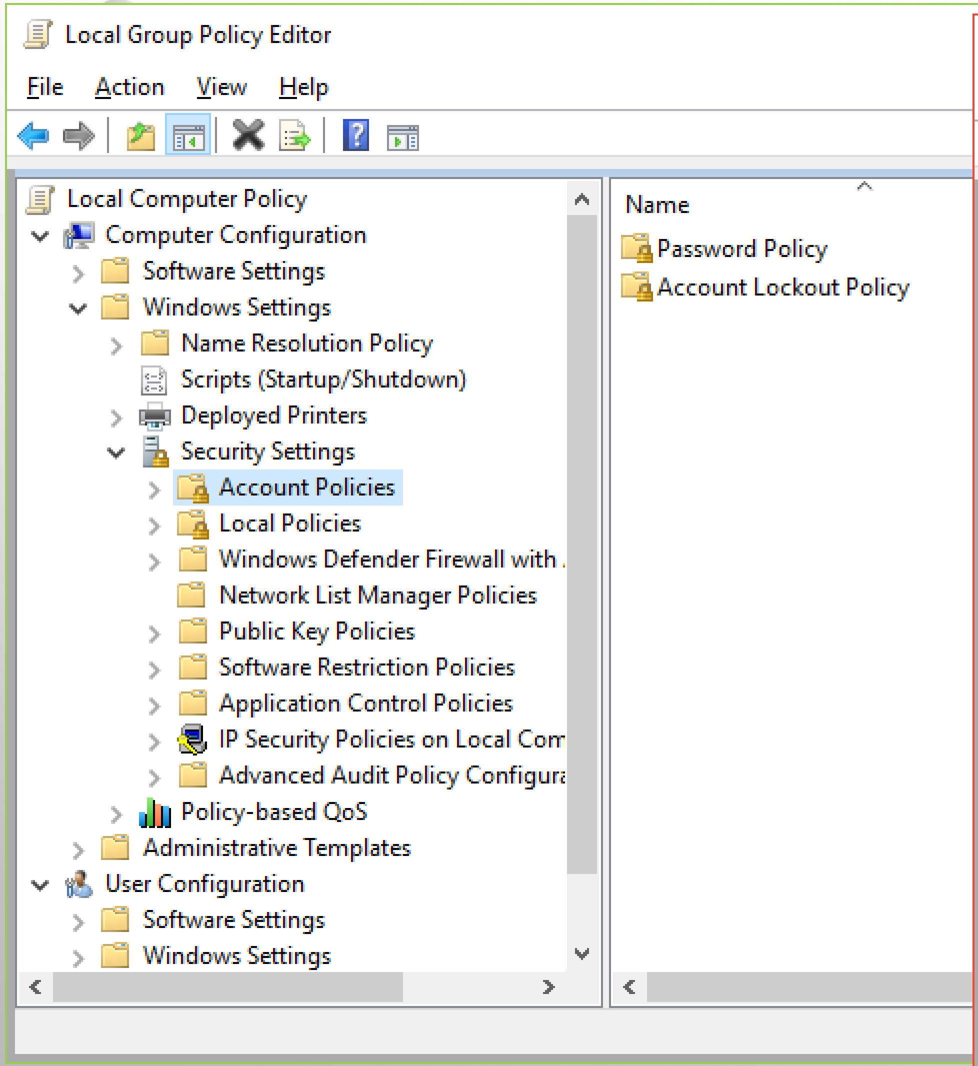
“SECURITY CONFIGURATION AND ANALYSIS” SNAP IN (4 STEP – RESULTS OF COMPARISON)



Policy	Database Setting	Computer Setting
Enforce password history	5 passwords reme...	0 passwords remembered
Maximum password age	Not Defined	42 days
Minimum password age	Not Defined	0 days
Minimum password length	3 characters	0 characters
Password must meet complexity requirements	Not Defined	Disabled
Store passwords using reversible encryption	Not Defined	Disabled

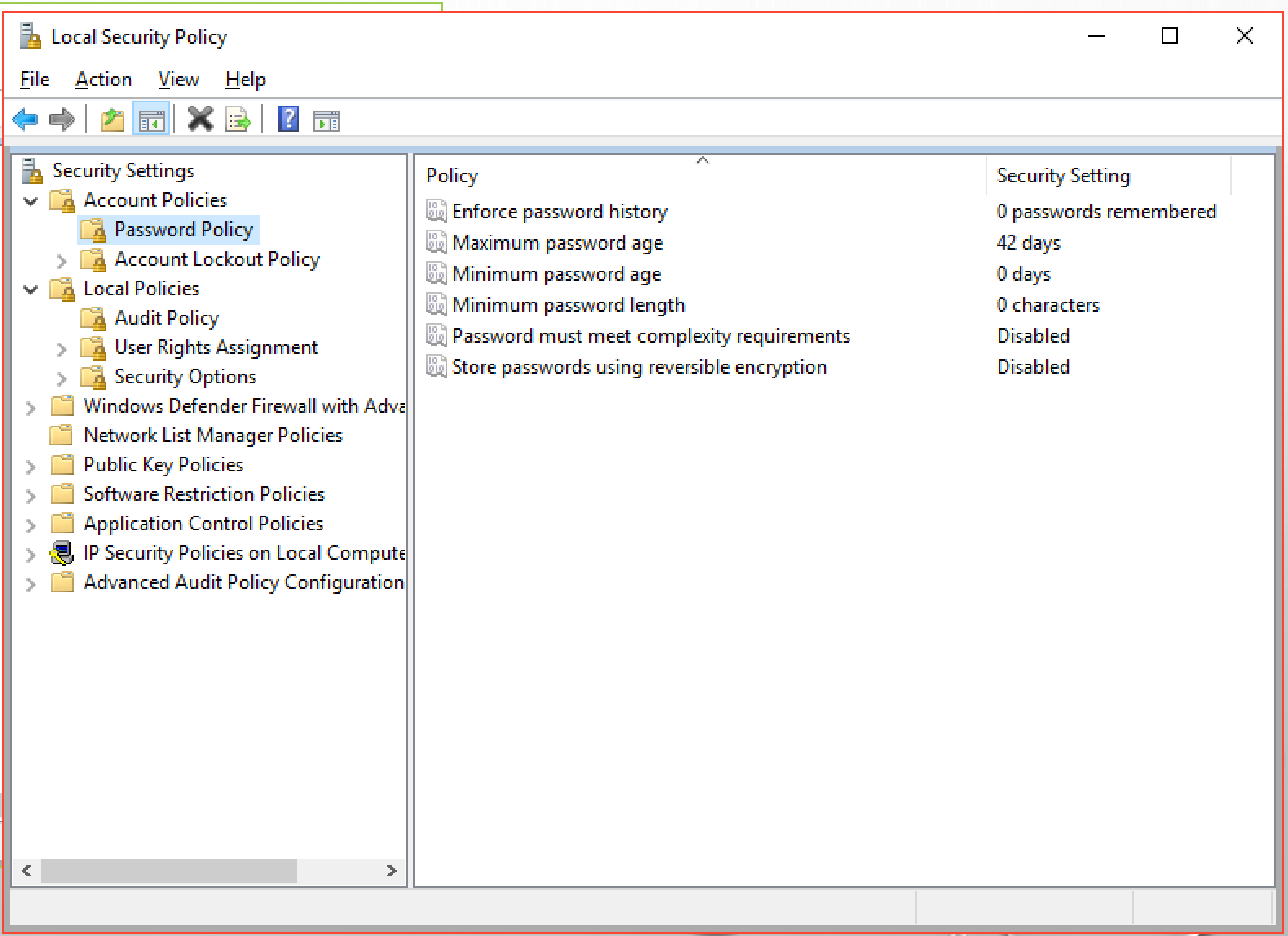
DIFFERENCIES BETWEEN THE TEMPLATE (DATABASE) AND LOCAL SECURITY POLICY OF THIS COMPUTER SYSTEM

LOCAL GROUP POLICY EDITOR



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Windows Defender Firewall with
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local Com
        - Advanced Audit Policy Configura
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings

Name
Password Policy
Account Lockout Policy



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

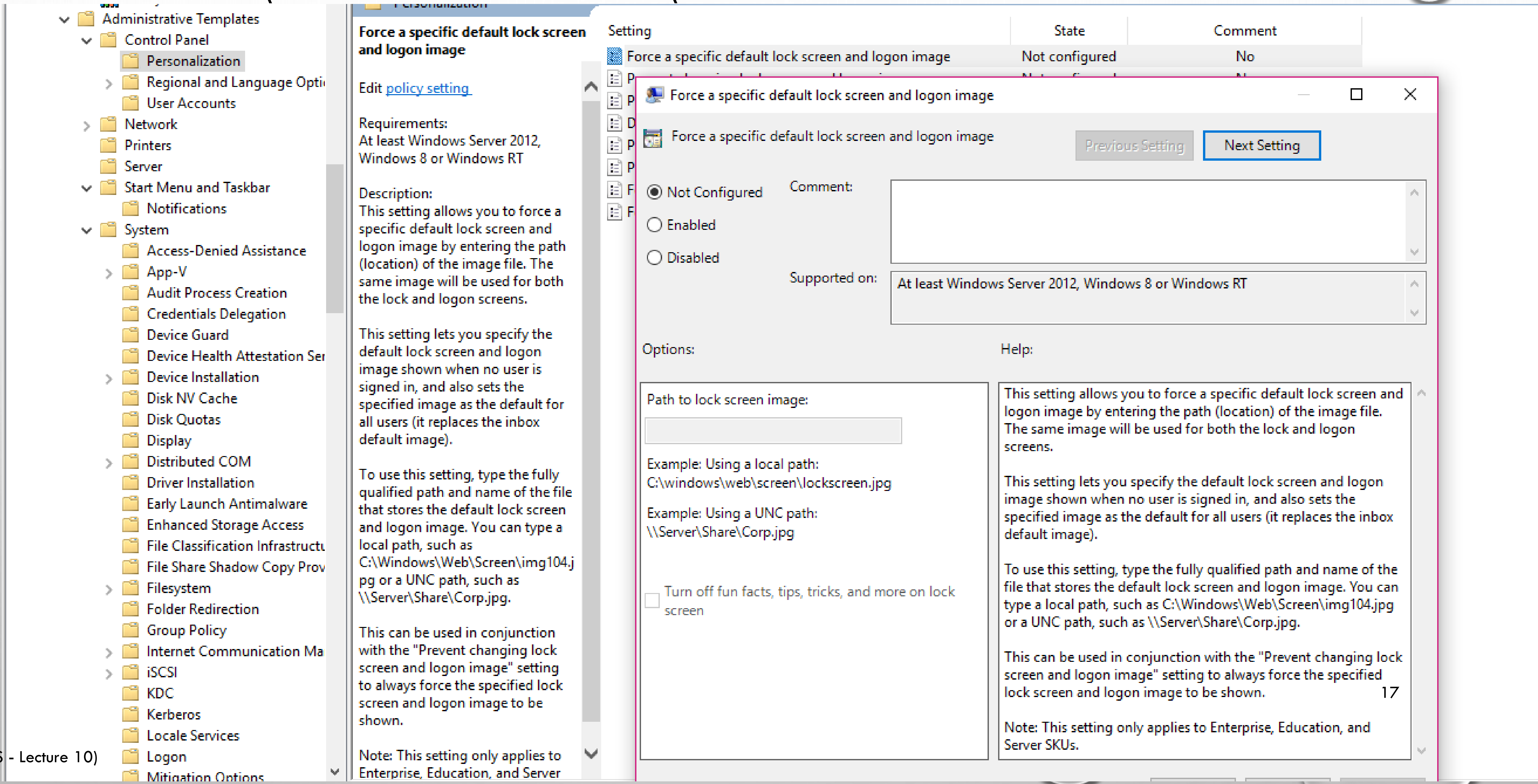
LOCAL GROUP POLICY EDITOR: TWO MAIN MODES (NODES)

- **COMPUTER CONFIGURATION**
  ADMINISTRATORS CAN USE COMPUTER CONFIGURATION TO SET POLICIES THAT ARE APPLIED TO COMPUTER, REGARDLESS OF WHO LOGS ON TO THE COMPUTERS. COMPUTER CONFIGURATION TYPICALLY CONTAINS SUB-ITEMS FOR SOFTWARE SETTINGS, WINDOWS SETTINGS, AND ADMINISTRATIVE TEMPLATES.
- **USER CONFIGURATION**
  ADMINISTRATORS CAN USE USER CONFIGURATION TO SET POLICIES THAT APPLY TO USERS, REGARDLESS OF WHICH COMPUTER THEY LOG ON TO. USER CONFIGURATION TYPICALLY CONTAINS SUB-ITEMS FOR SOFTWARE SETTINGS, WINDOWS SETTINGS, AND ADMINISTRATIVE TEMPLATES.

LOCAL GROUP POLICY EDITOR

- *THE “SOFTWARE SETTINGS*” NODE IS USED TO ADD SOFTWARE APPLICATION PACKAGES TO THE COMPUTERS THAT PROCESS THE PARTICULAR POLICY.
- THE “SECURITY SETTINGS: THIS NODE IS A REPLICA OF THE LOCAL SECURITY POLICY, ALTHOUGH IT DOES NOT SYNC OR PULL INFORMATION FROM THE LOCAL SECURITY POLICY.
- THE “COMPUTER CONFIGURATION ADMINISTRATIVE TEMPLATES” NODE CONTAINS ALL OF THE REGISTRY BASED POLICY SETTINGS THAT APPLY TO THE WINDOWS SYSTEM. THESE SETTINGS ARE PRIMARILY USED TO CONTROL, CONFIGURE, AND SECURE HOW THE WINDOWS SYSTEM IS SET UP AND HOW IT CAN BE USED.

LOCAL GROUP POLICY EDITOR\ADMINISTRATIVE TEMPLATES\PERSONALIZATION\DEFAULT LOCK SCREEN SETTING



Force a specific default lock screen and logon image

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This setting allows you to force a specific default lock screen and logon image by entering the path (location) of the image file. The same image will be used for both the lock and logon screens.

This setting lets you specify the default lock screen and logon image shown when no user is signed in, and also sets the specified image as the default for all users (it replaces the inbox default image).

To use this setting, type the fully qualified path and name of the file that stores the default lock screen and logon image. You can type a local path, such as C:\Windows\Web\Screen\img104.jpg or a UNC path, such as \\Server\Share\Corp.jpg.

This can be used in conjunction with the "Prevent changing lock screen and logon image" setting to always force the specified lock screen and logon image to be shown.

Note: This setting only applies to Enterprise, Education, and Server

Setting	State	Comment
Force a specific default lock screen and logon image	Not configured	No

Force a specific default lock screen and logon image

Force a specific default lock screen and logon image

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Path to lock screen image:

Example: Using a local path:
C:\windows\web\screen\lockscreen.jpg

Example: Using a UNC path:
\\Server\Share\Corp.jpg

☐ Turn off fun facts, tips, tricks, and more on lock screen

Help:

This setting allows you to force a specific default lock screen and logon image by entering the path (location) of the image file. The same image will be used for both the lock and logon screens.

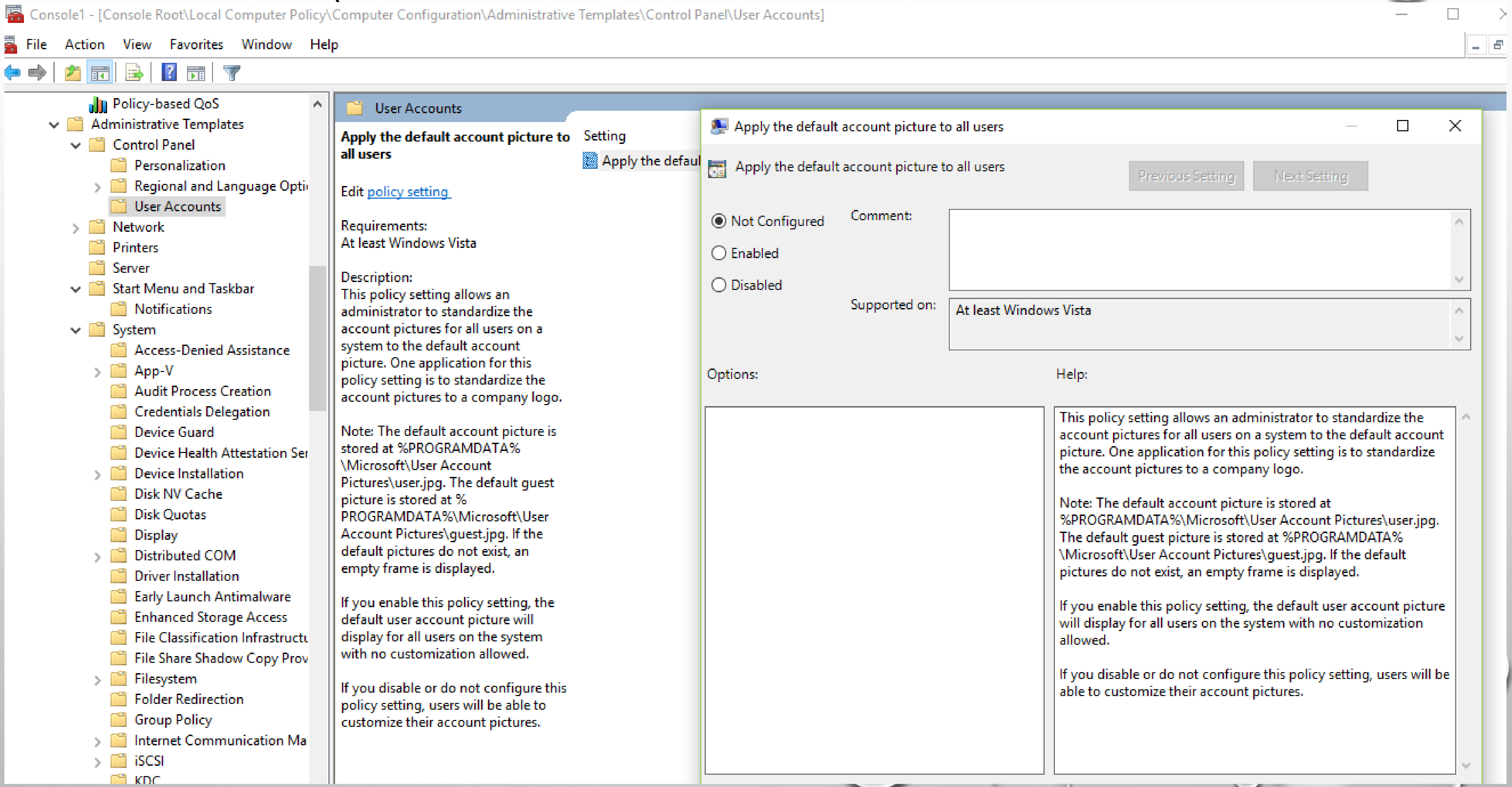
This setting lets you specify the default lock screen and logon image shown when no user is signed in, and also sets the specified image as the default for all users (it replaces the inbox default image).

To use this setting, type the fully qualified path and name of the file that stores the default lock screen and logon image. You can type a local path, such as C:\Windows\Web\Screen\img104.jpg or a UNC path, such as \\Server\Share\Corp.jpg.

This can be used in conjunction with the "Prevent changing lock screen and logon image" setting to always force the specified lock screen and logon image to be shown.

Note: This setting only applies to Enterprise, Education, and Server SKUs.

LOCAL GROUP POLICY EDITOR\ADMINISTRATIVE TEMPLATES\USER ACCOUNTS\ACCOUNT PICTURES STANDARDIZATION



Apply the default account picture to all users

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows an administrator to standardize the account pictures for all users on a system to the default account picture. One application for this policy setting is to standardize the account pictures to a company logo.

Note: The default account picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\user.jpg. The default guest picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\guest.jpg. If the default pictures do not exist, an empty frame is displayed.

If you enable this policy setting, the default user account picture will display for all users on the system with no customization allowed.

If you disable or do not configure this policy setting, users will be able to customize their account pictures.

Apply the default account picture to all users

Apply the default account picture to all users

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

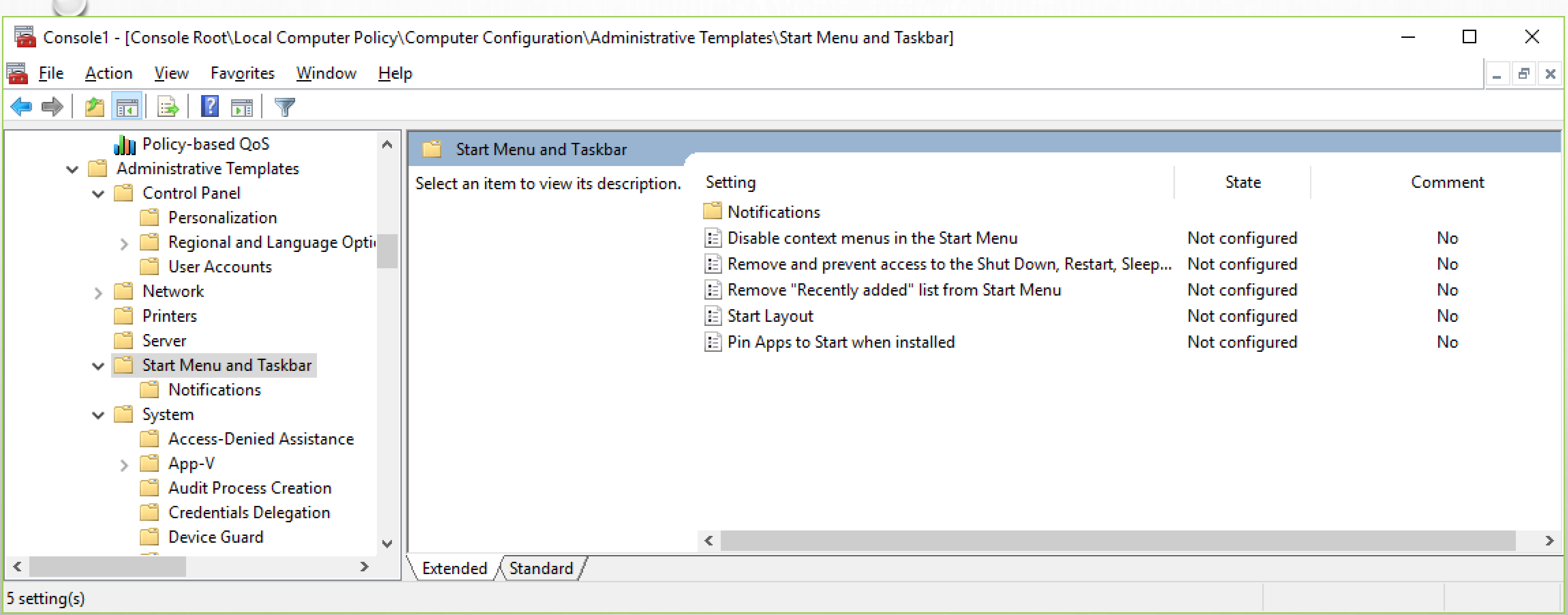
This policy setting allows an administrator to standardize the account pictures for all users on a system to the default account picture. One application for this policy setting is to standardize the account pictures to a company logo.

Note: The default account picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\user.jpg. The default guest picture is stored at %PROGRAMDATA%\Microsoft\User Account Pictures\guest.jpg. If the default pictures do not exist, an empty frame is displayed.

If you enable this policy setting, the default user account picture will display for all users on the system with no customization allowed.

If you disable or do not configure this policy setting, users will be able to customize their account pictures.

LOCAL GROUP POLICY EDITOR\ADMINISTRATIVE TEMPLATES\START MENU AND TASKBAR



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Start Menu and Taskbar]

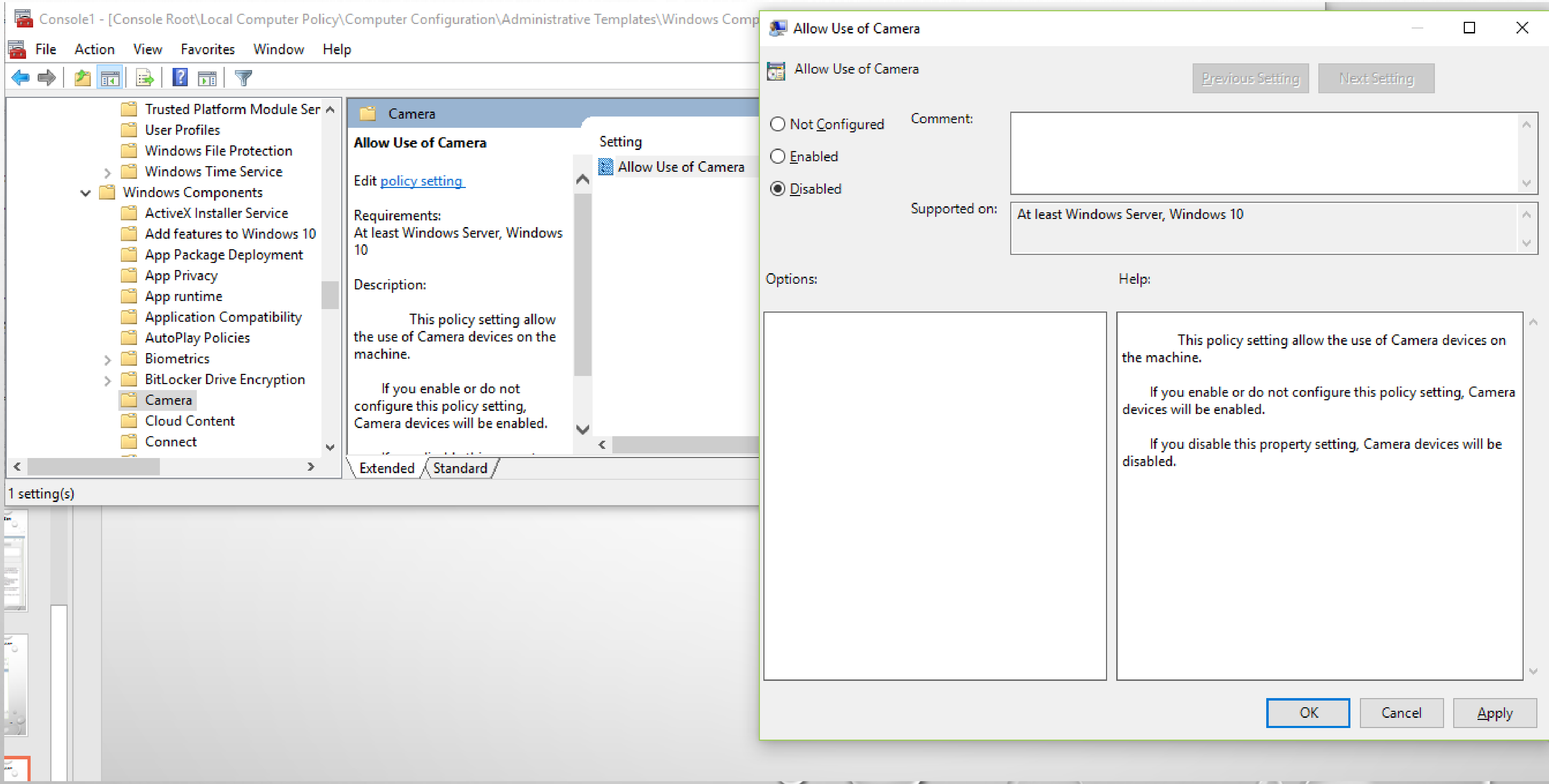
Start Menu and Taskbar

Select an item to view its description.

Setting	State	Comment
Notifications		
Disable context menus in the Start Menu	Not configured	No
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured	No
Remove "Recently added" list from Start Menu	Not configured	No
Start Layout	Not configured	No
Pin Apps to Start when installed	Not configured	No

5 setting(s)

LOCAL GROUP POLICY EDITOR\ADMINISTRATIVE TEMPLATES\WINDOWS COMPONENTS \CAMERA



Allow Use of Camera

Edit policy setting

Requirements:
At least Windows Server, Windows 10

Description:

This policy setting allow the use of Camera devices on the machine.

If you enable or do not configure this policy setting, Camera devices will be enabled.

Allow Use of Camera

○ Not Configured
○ Enabled
● Disabled

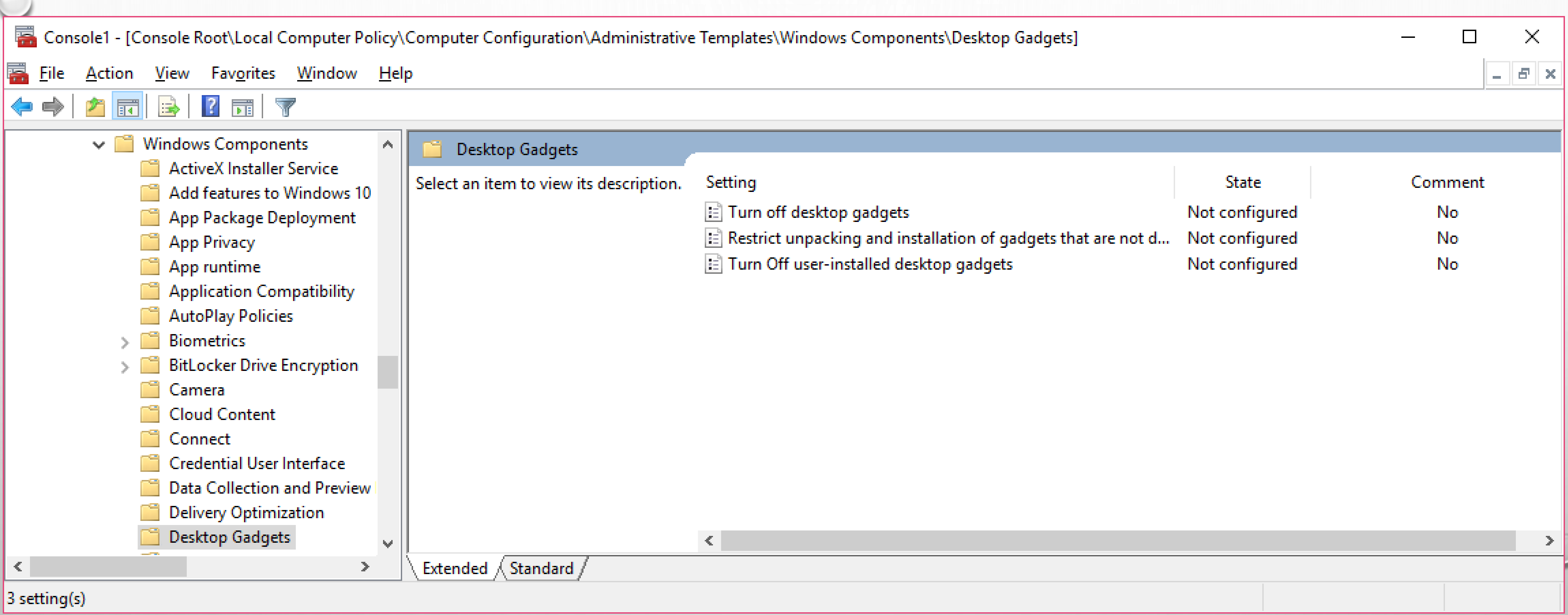
Supported on: At least Windows Server, Windows 10

This policy setting allow the use of Camera devices on the machine.

If you enable or do not configure this policy setting, Camera devices will be enabled.

If you disable this property setting, Camera devices will be disabled.

LOCAL GROUP POLICY EDITOR\ADMINISTRATIVE TEMPLATES\WINDOWS COMPONENTS \DESKTOP GADGETS



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Desktop Gadgets]

Desktop Gadgets

Select an item to view its description.

Setting	State	Comment
Turn off desktop gadgets	Not configured	No
Restrict unpacking and installation of gadgets that are not d...	Not configured	No
Turn Off user-installed desktop gadgets	Not configured	No

3 setting(s)

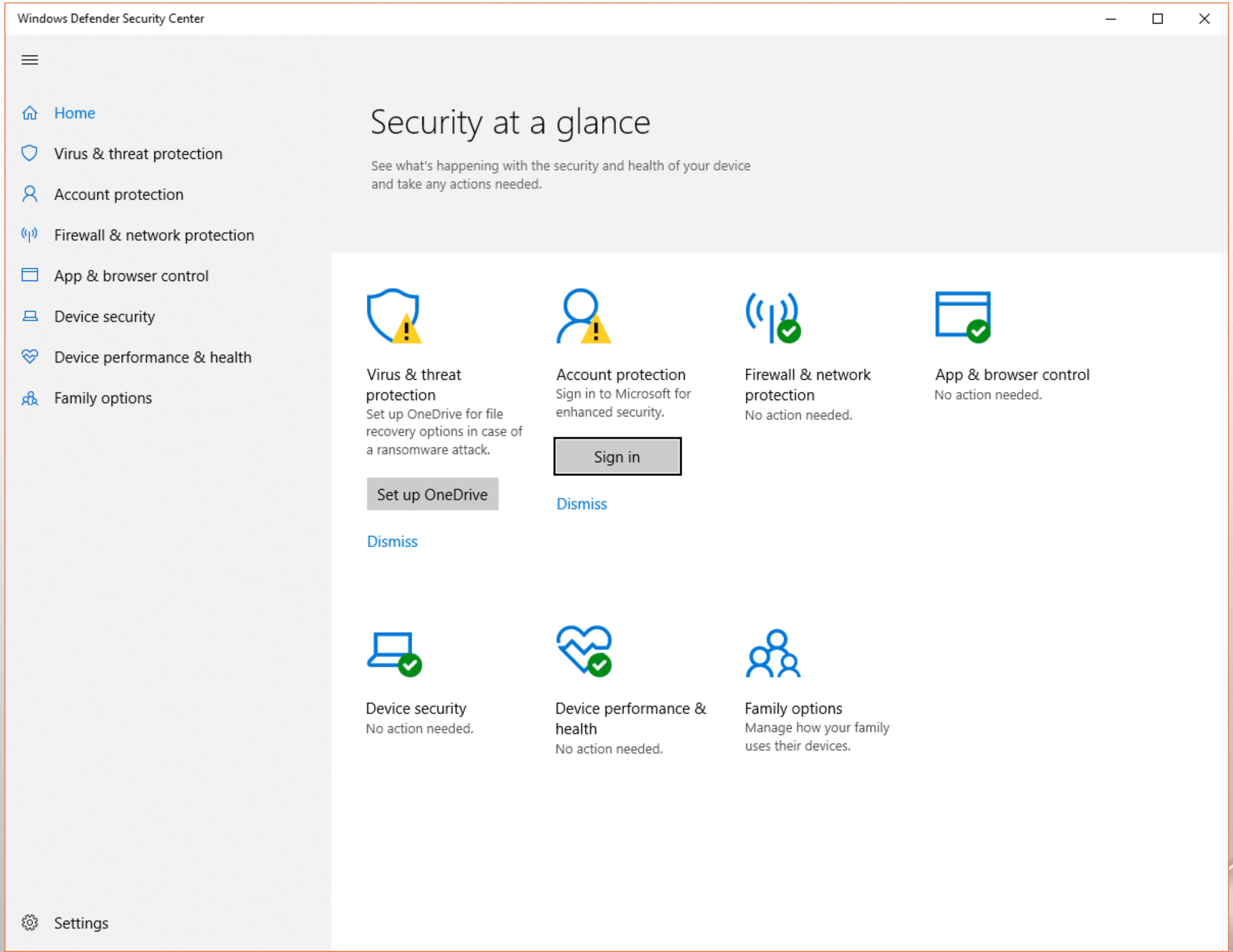
SECURITY SUBSYSTEM IN WINDOWS

OTHER SECURITY TOOLS

WINDOWS DEFENDER

- **WINDOWS DEFENDER** (KNOWN AS **WINDOWS DEFENDER ANTIVIRUS**) IS AN ANTI-MALWARE COMPONENT OF MICROSOFT WINDOWS.
- IT WAS FIRST RELEASED AS A DOWNLOADABLE FREE ANTISPYWARE PROGRAM FOR WINDOWS XP, AND WAS LATER SHIPPED WITH WINDOWS VISTA AND WINDOWS 7.
- IT HAS EVOLVED INTO A FULL ANTIVIRUS PROGRAM, REPLACING MICROSOFT SECURITY ESSENTIALS AS PART OF WINDOWS 8 AND LATER VERSIONS.
- BEFORE WINDOWS 8, WINDOWS DEFENDER ONLY PROTECTED USERS AGAINST SPYWARE. IT INCLUDES A NUMBER OF REAL-TIME SECURITY AGENTS THAT MONITOR SEVERAL COMMON AREAS OF WINDOWS FOR CHANGES WHICH MIGHT HAVE BEEN CAUSED BY SPYWARE. PROTECTION AGAINST VIRUSES WAS SUBSEQUENTLY ADDED IN WINDOWS 8; WHICH RESEMBLES MICROSOFT SECURITY ESSENTIALS (MSE).
- IN WINDOWS 10, WINDOWS DEFENDER SETTINGS ARE CONTROLLED IN THE WINDOWS DEFENDER SECURITY CENTER.

WINDOWS DEFENDER SECURITY CENTER


Windows Defender Security Center
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
Set up OneDrive for file recovery options in case of a ransomware attack.

Account protection
Sign in to Microsoft for enhanced security.

Firewall & network protection
No action needed.

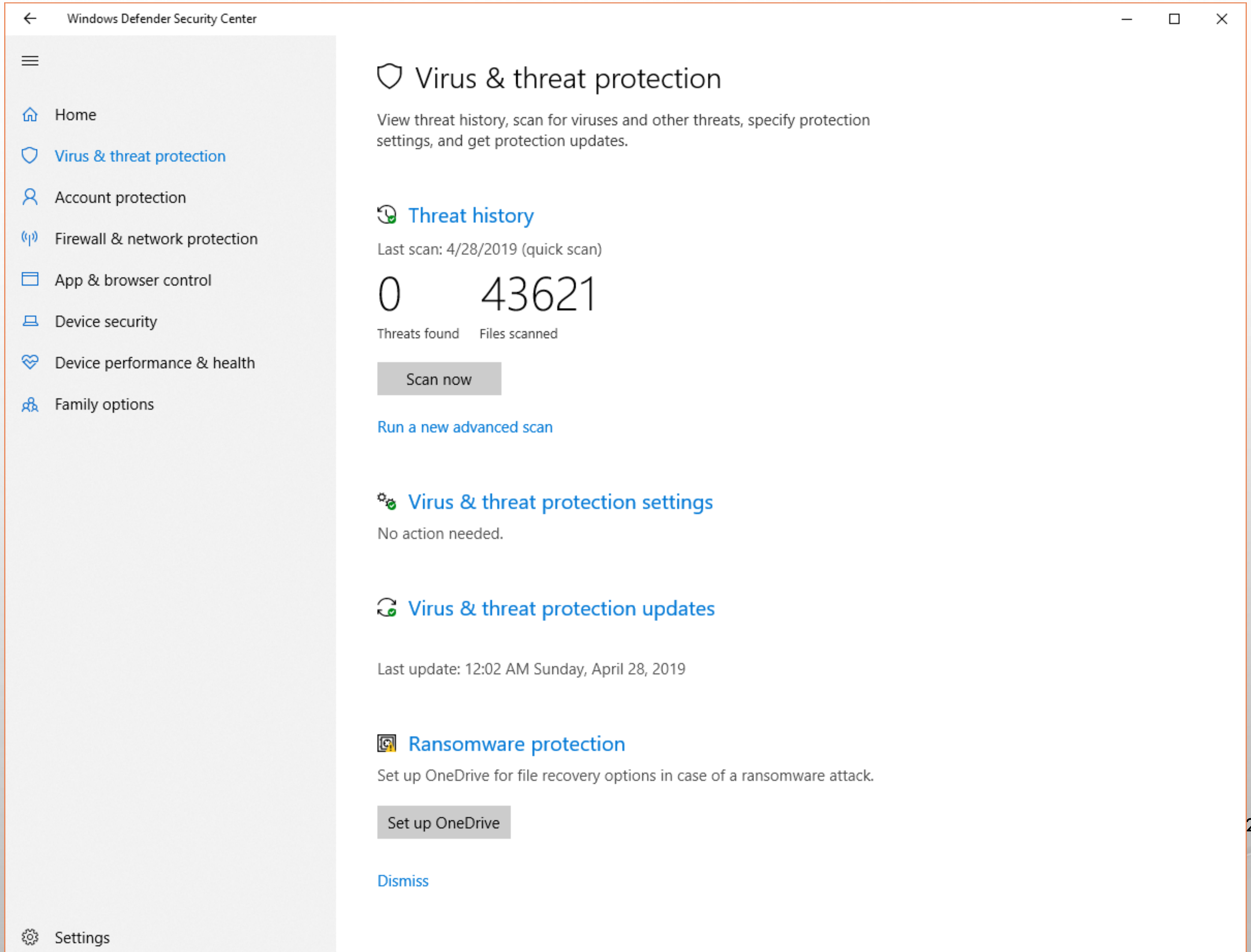
App & browser control
No action needed.

Device security
No action needed.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

VIRUS & THREAT PROTECTION



Windows Defender Security Center
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

Threat history

Last scan: 4/28/2019 (quick scan)

0 Threats found

43621 Files scanned

Scan now

Run a new advanced scan

Virus & threat protection settings

No action needed.

Virus & threat protection updates

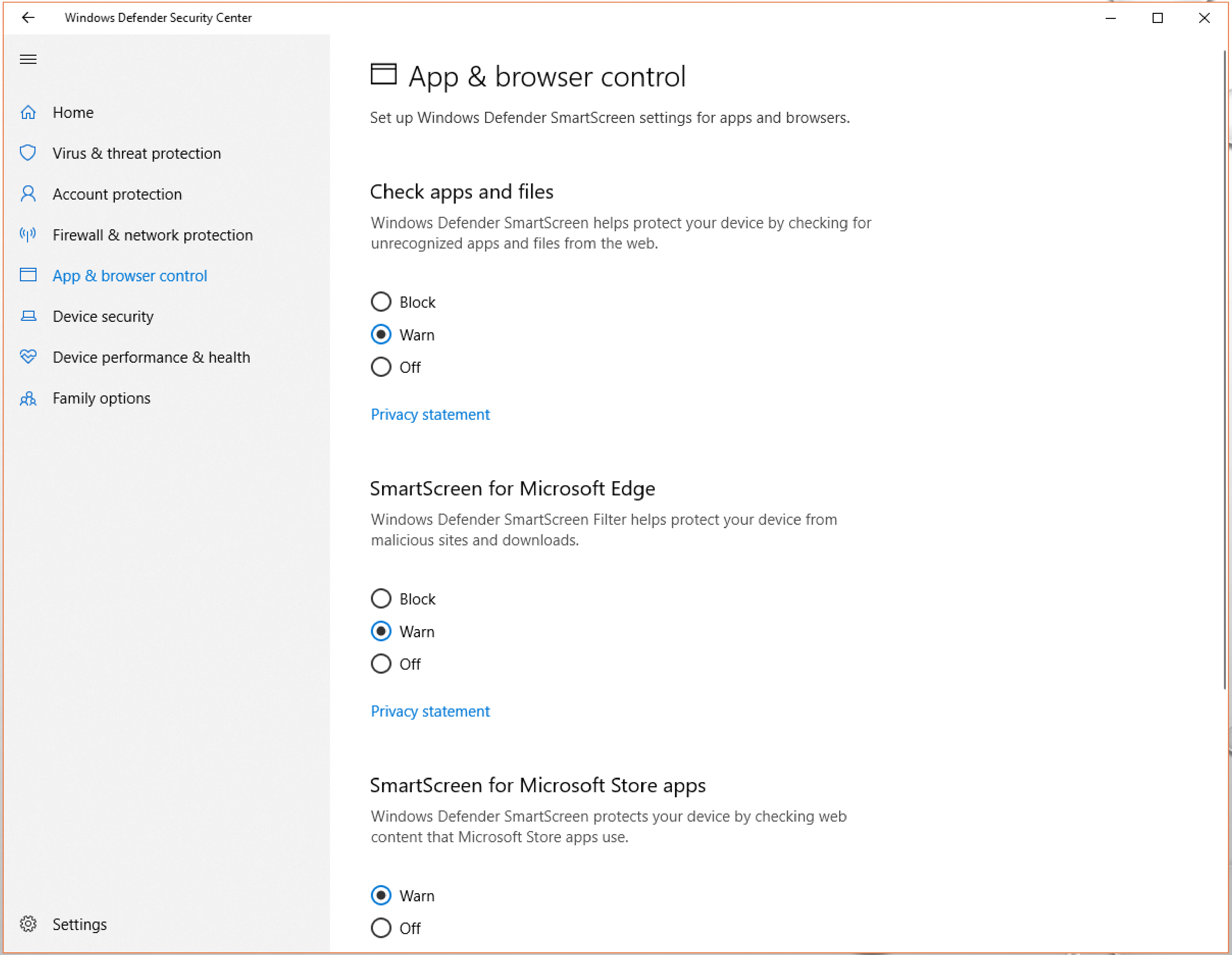
Last update: 12:02 AM Sunday, April 28, 2019

Ransomware protection

Set up OneDrive for file recovery options in case of a ransomware attack.

Set up OneDrive

Dismiss


Windows Defender Security Center
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

App & browser control

Set up Windows Defender SmartScreen settings for apps and browsers.

Check apps and files

Windows Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

○ Block
● Warn
○ Off

Privacy statement

SmartScreen for Microsoft Edge

Windows Defender SmartScreen Filter helps protect your device from malicious sites and downloads.

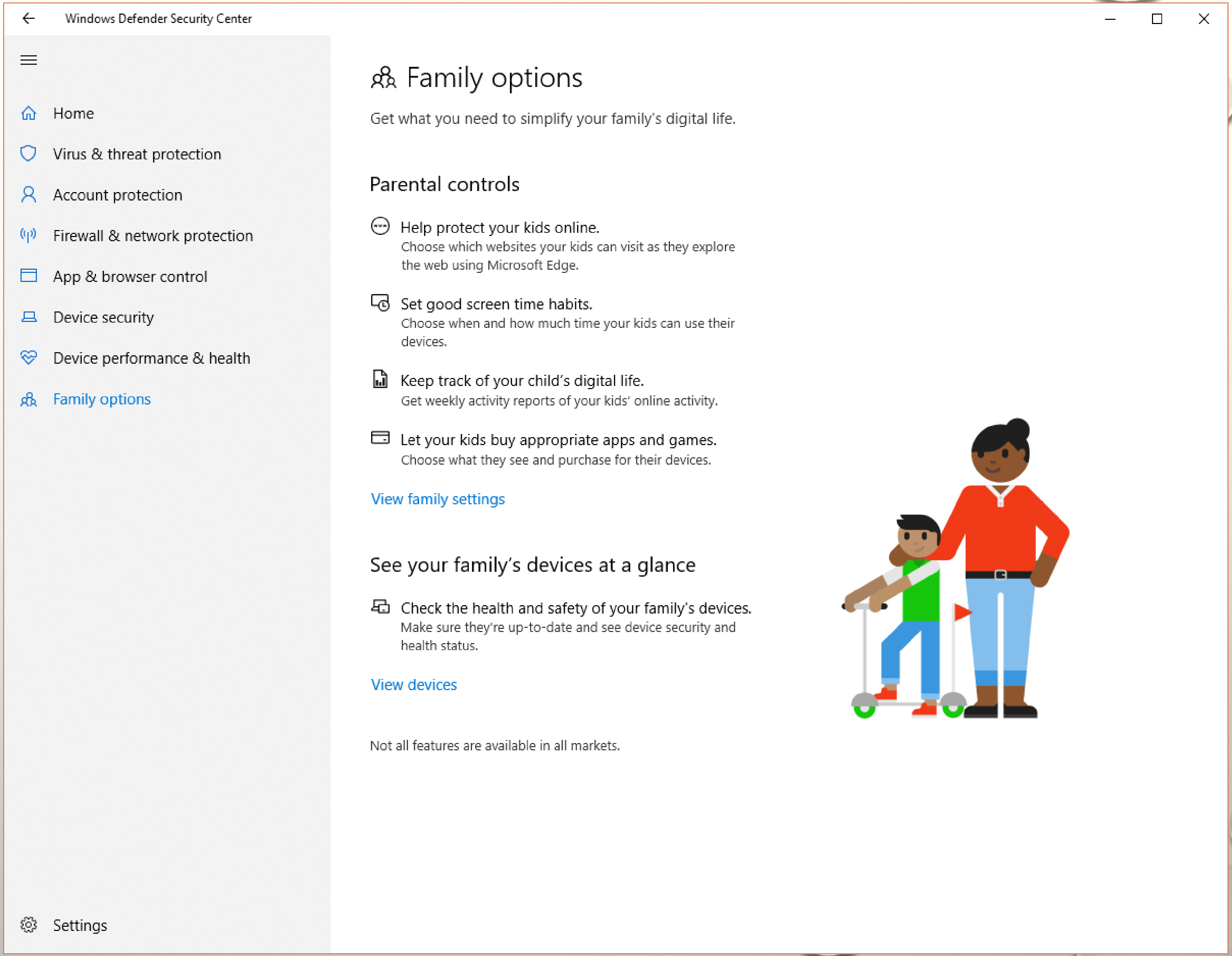
○ Block
● Warn
○ Off

Privacy statement

SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.

● Warn
○ Off



Windows Defender Security Center
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

Family options

Get what you need to simplify your family's digital life.

Parental controls

Help protect your kids online.
Choose which websites your kids can visit as they explore the web using Microsoft Edge.

Set good screen time habits.
Choose when and how much time your kids can use their devices.

Keep track of your child's digital life.
Get weekly activity reports of your kids' online activity.

Let your kids buy appropriate apps and games.
Choose what they see and purchase for their devices.

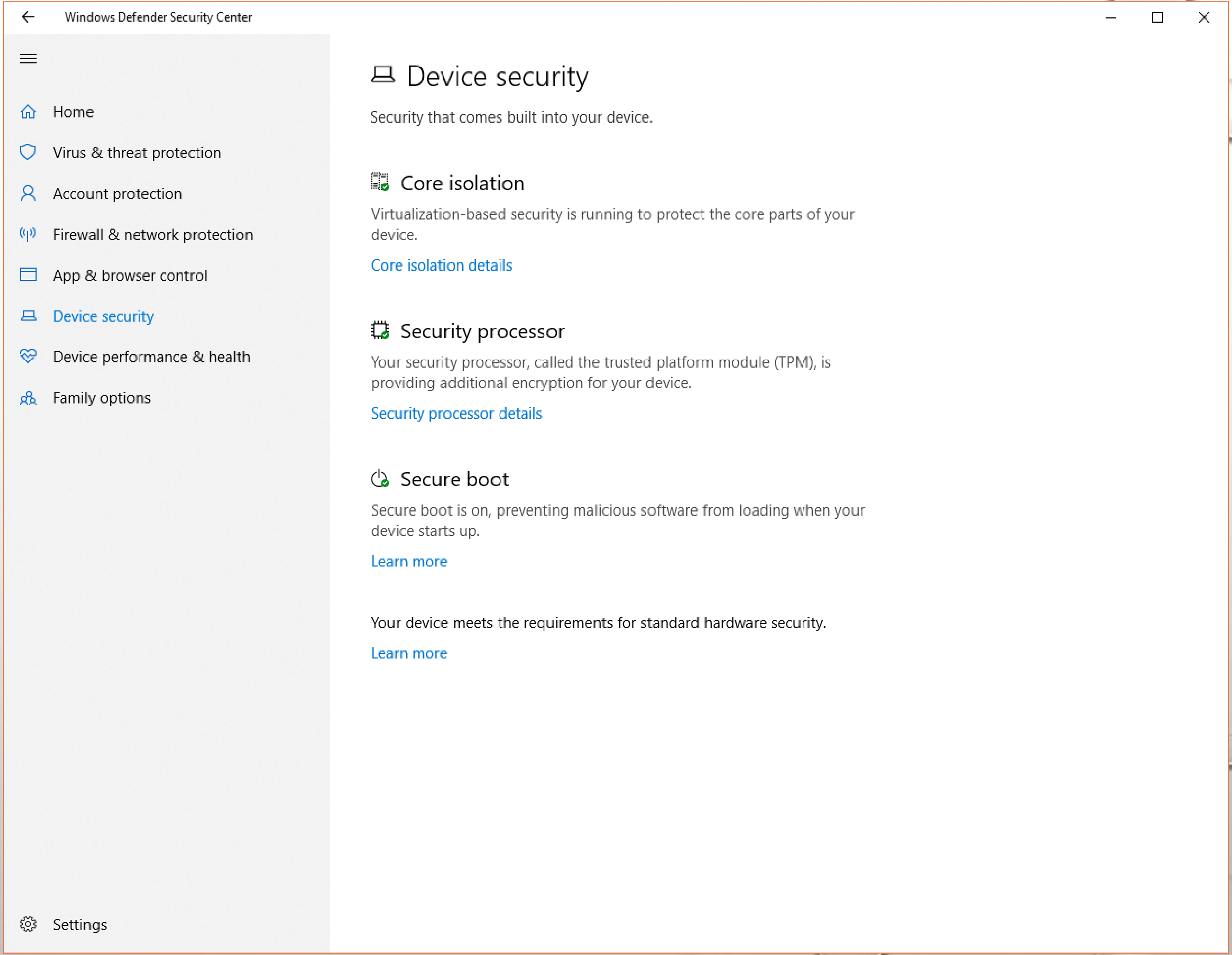
View family settings

See your family's devices at a glance

Check the health and safety of your family's devices.
Make sure they're up-to-date and see device security and health status.

View devices

Not all features are available in all markets.



Windows Defender Security Center
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings

Device security

Security that comes built into your device.

Core isolation

Virtualization-based security is running to protect the core parts of your device.

Core isolation details

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

Security processor details

Secure boot

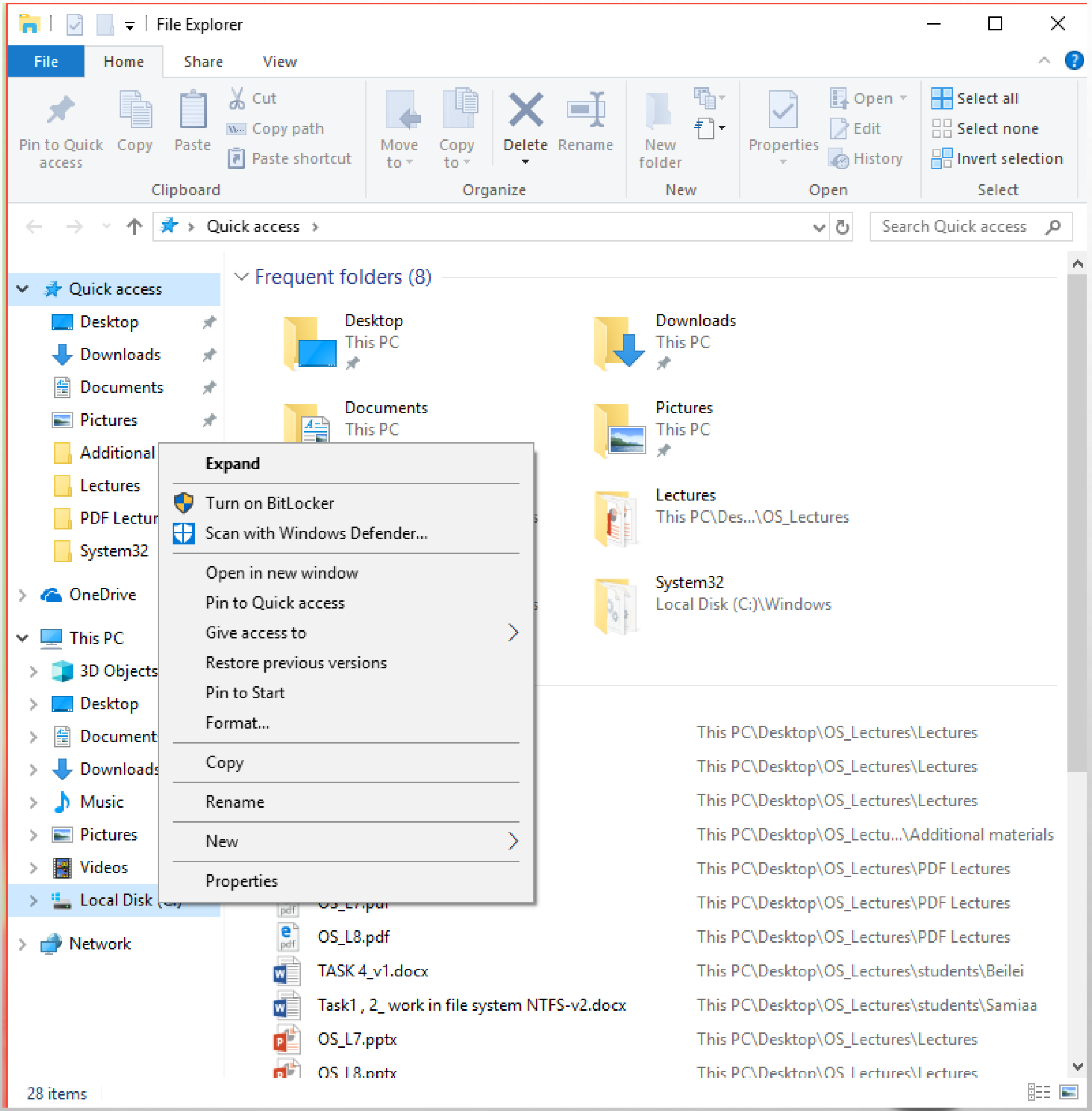
Secure boot is on, preventing malicious software from loading when your device starts up.

Learn more

Your device meets the requirements for standard hardware security.

Learn more

DEFENDER SCANNING START



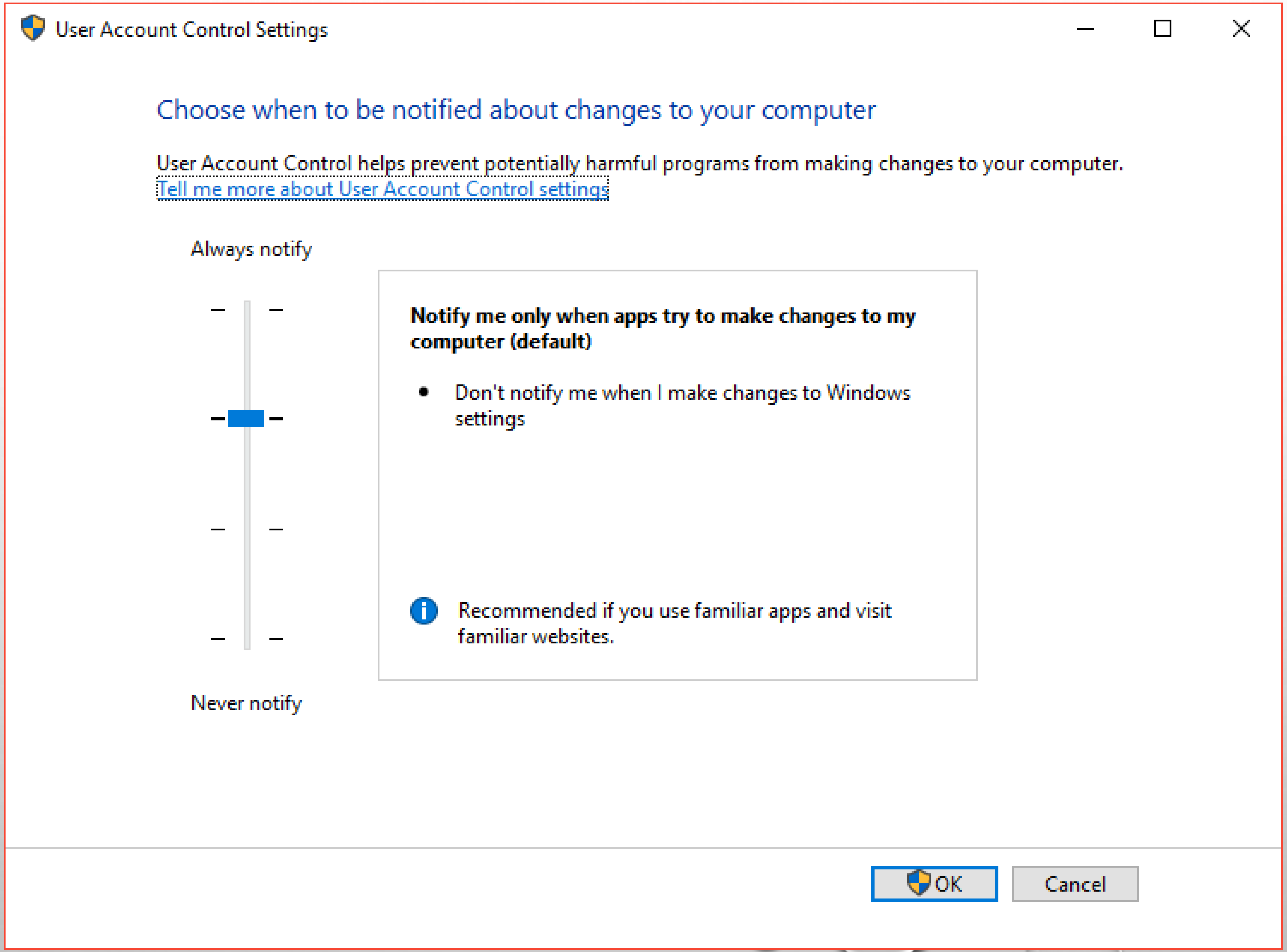
This PC\Desktop\OS_Lectures\Lectures
This PC\Desktop\OS_Lectures\Lectures
This PC\Desktop\OS_Lectures\Lectures
This PC\Desktop\OS_Lectu...\Additional materials
This PC\Desktop\OS_Lectures\PDF Lectures

OS_L7.pdf	This PC\Desktop\OS_Lectures\PDF Lectures
OS_L8.pdf	This PC\Desktop\OS_Lectures\PDF Lectures
TASK 4_v1.docx	This PC\Desktop\OS_Lectures\students\Beilei
Task1 , 2_ work in file system NTFS-v2.docx	This PC\Desktop\OS_Lectures\students\Samiaa
OS_L7.pptx	This PC\Desktop\OS_Lectures\Lectures
OS_L8.pptx	This PC\Desktop\OS_Lectures\Lectures

USER ACCOUNT CONTROL (UAC)

- UAC HELPS PREVENT MALWARE FROM SILENTLY INSTALLING WITHOUT AN ADMINISTRATOR'S KNOWLEDGE.
- UAC ALLOWS ALL USERS TO LOG ON TO THEIR COMPUTERS USING A STANDARD USER ACCOUNT. PROCESSES LAUNCHED USING A STANDARD USER TOKEN MAY PERFORM TASKS USING ACCESS RIGHTS GRANTED TO A STANDARD USER. FOR INSTANCE, WINDOWS EXPLORER AUTOMATICALLY INHERITS STANDARD USER LEVEL PERMISSIONS. ADDITIONALLY, ANY APPS THAT ARE STARTED USING WINDOWS EXPLORER (FOR EXAMPLE, BY DOUBLE-CLICKING A SHORTCUT) ALSO RUN WITH THE STANDARD SET OF USER PERMISSIONS. MANY APPS, INCLUDING THOSE THAT ARE INCLUDED WITH THE OPERATING SYSTEM ITSELF, ARE DESIGNED TO WORK PROPERLY IN THIS WAY.
- OTHER APPS, ESPECIALLY THOSE THAT WERE NOT SPECIFICALLY DESIGNED WITH SECURITY SETTINGS IN MIND, OFTEN REQUIRE ADDITIONAL PERMISSIONS TO RUN SUCCESSFULLY. THESE TYPES OF APPS ARE REFERRED TO AS LEGACY APPS. ADDITIONALLY, ACTIONS SUCH AS INSTALLING NEW SOFTWARE AND MAKING CONFIGURATION CHANGES TO THE WINDOWS FIREWALL, REQUIRE MORE PERMISSIONS THAN WHAT IS AVAILABLE TO A STANDARD USER ACCOUNT.

UAC



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

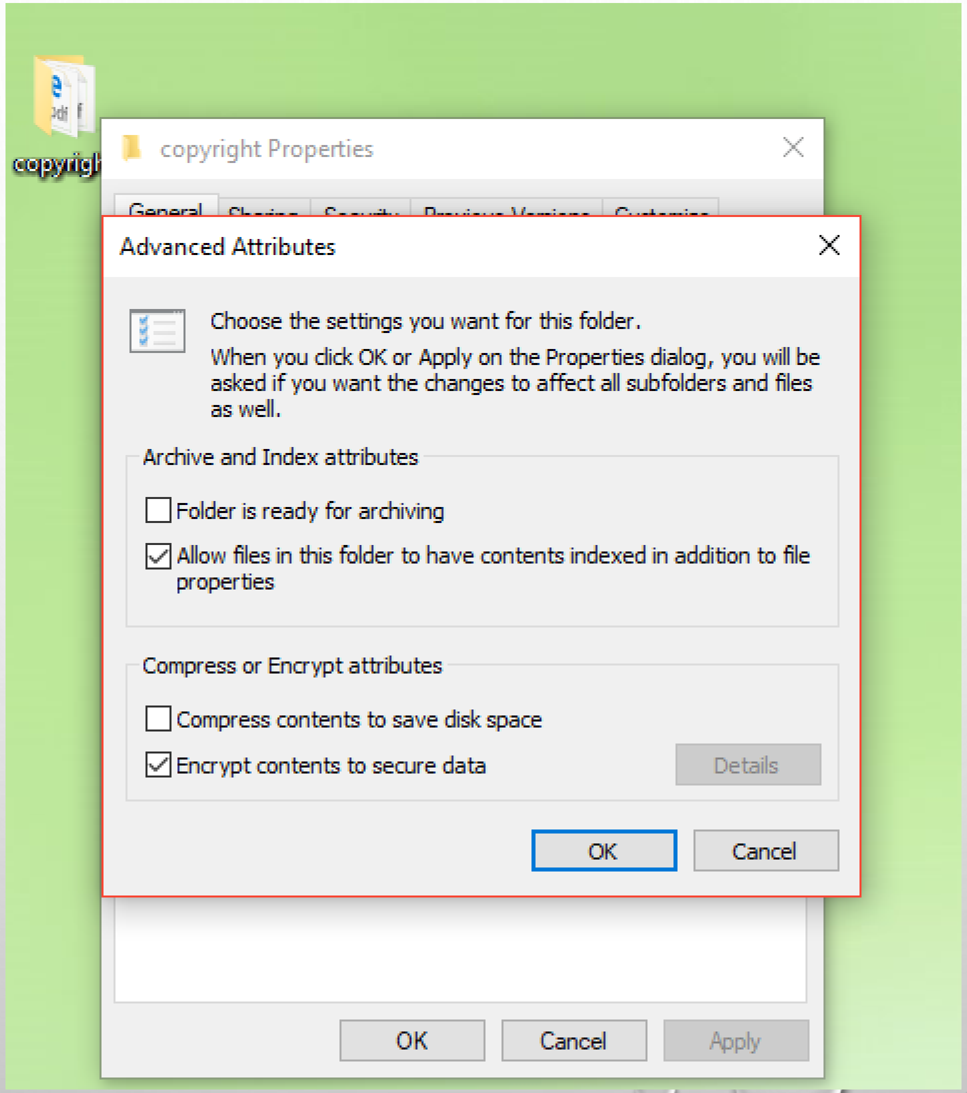
Recommended if you use familiar apps and visit familiar websites.

Never notify

ENCRYPTION: EFS & BITLOCKER

- EFS: IT IS POSSIBLE TO ENCRYPT SINGLE (OR SEVERAL) FILE AND/OR FOLDER
- BITLOCKER: THE ENTIRE DISK IS ENCRYPTED

EFS (ENCRYPTED FILE SYSTEM)



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

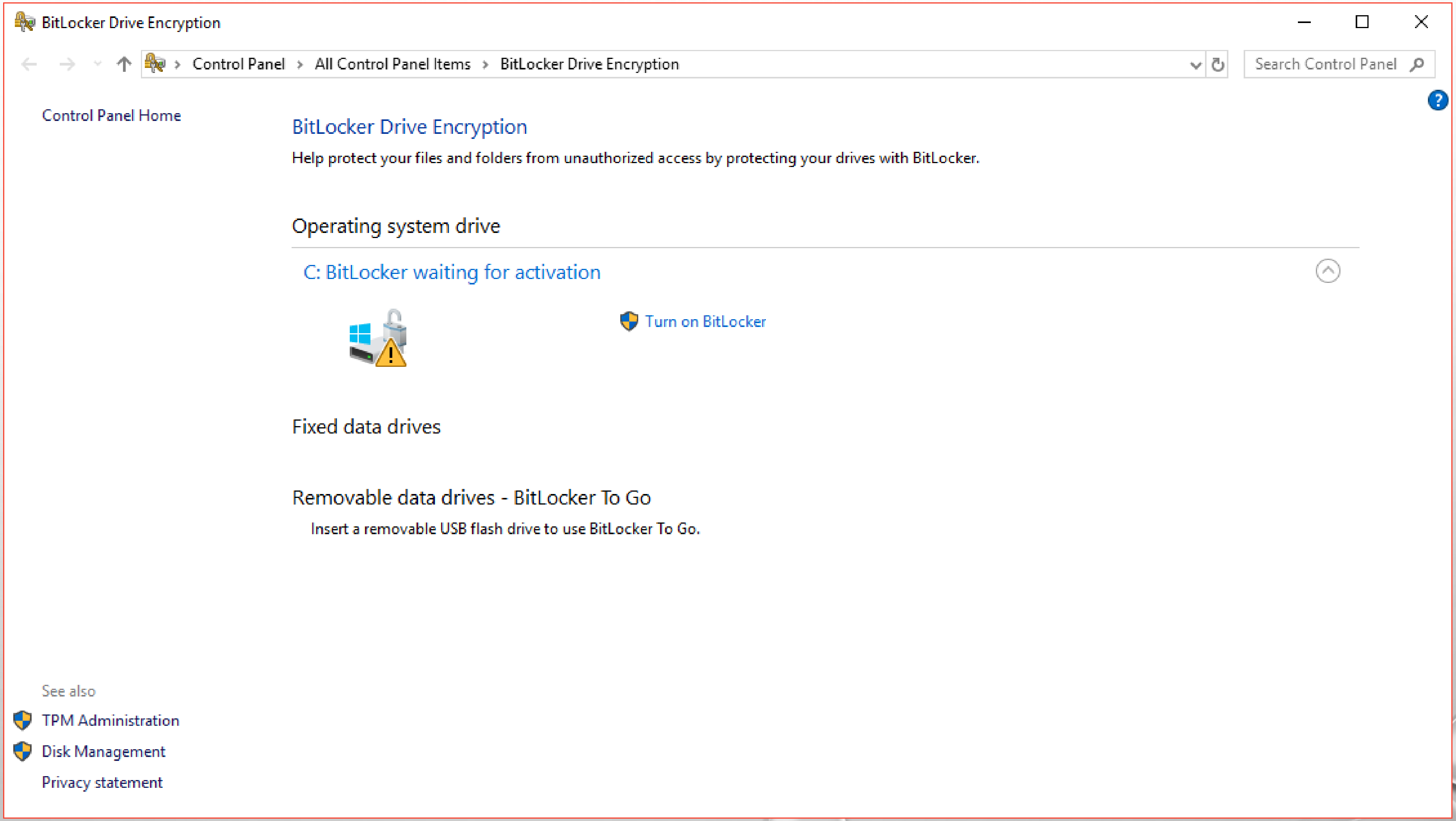
☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

BITLOCKER



BitLocker Drive Encryption
Control Panel › All Control Panel Items › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker waiting for activation

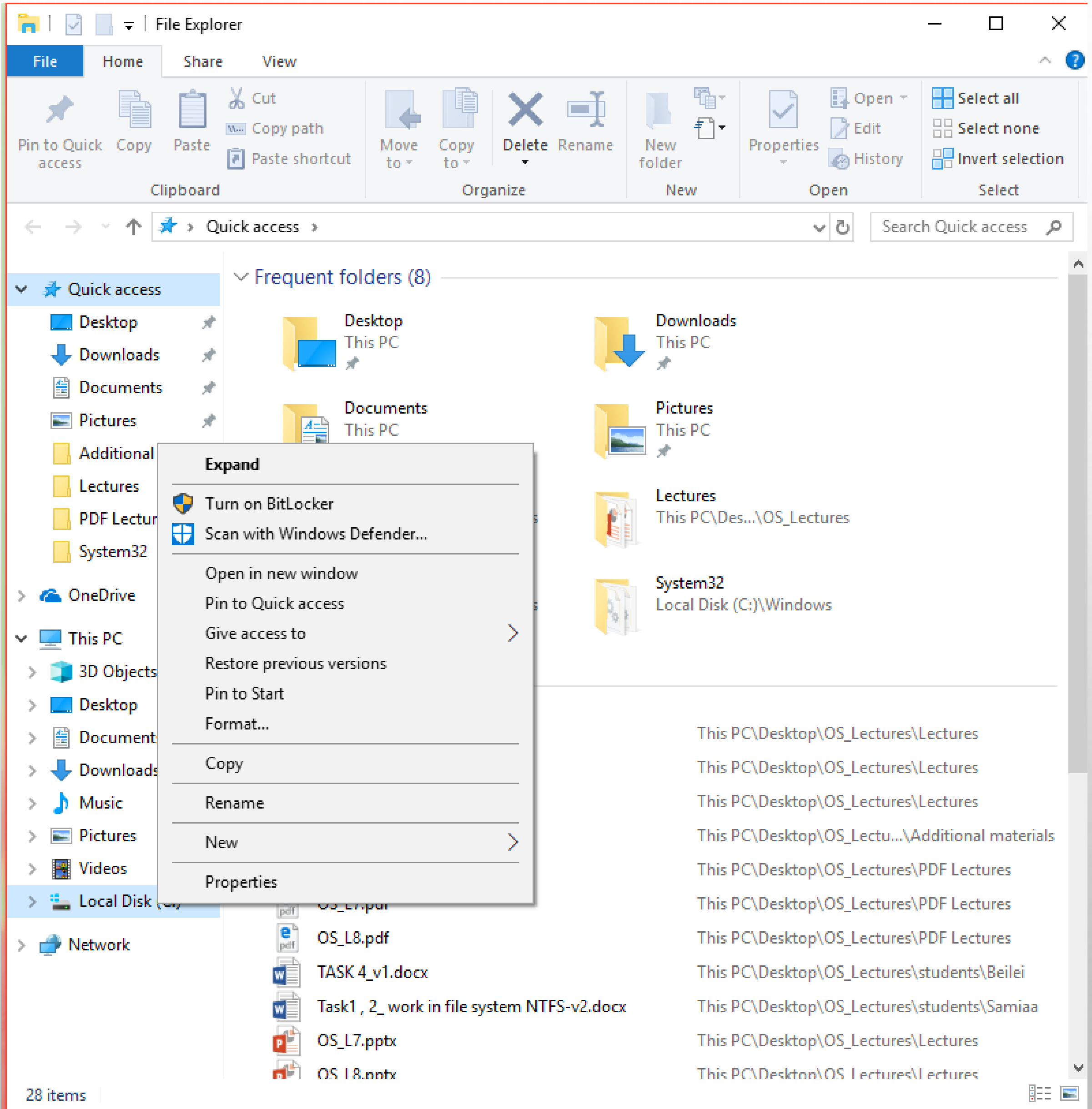
Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

BITLOCKER



	This PC\Desktop\OS_Lectures\Lectures
	This PC\Desktop\OS_Lectures\Lectures
	This PC\Desktop\OS_Lectures\Lectures
	This PC\Desktop\OS_Lectu...\Additional materials
	This PC\Desktop\OS_Lectures\PDF Lectures
OS_L7.pdf	This PC\Desktop\OS_Lectures\PDF Lectures
OS_L8.pdf	This PC\Desktop\OS_Lectures\PDF Lectures
TASK 4_v1.docx	This PC\Desktop\OS_Lectures\students\Beilei
Task1 , 2_ work in file system NTFS-v2.docx	This PC\Desktop\OS_Lectures\students\Samiaa
OS_L7.pptx	This PC\Desktop\OS_Lectures\Lectures
OS_L8.pptx	This PC\Desktop\OS_Lectures\Lectures

HOME TASK

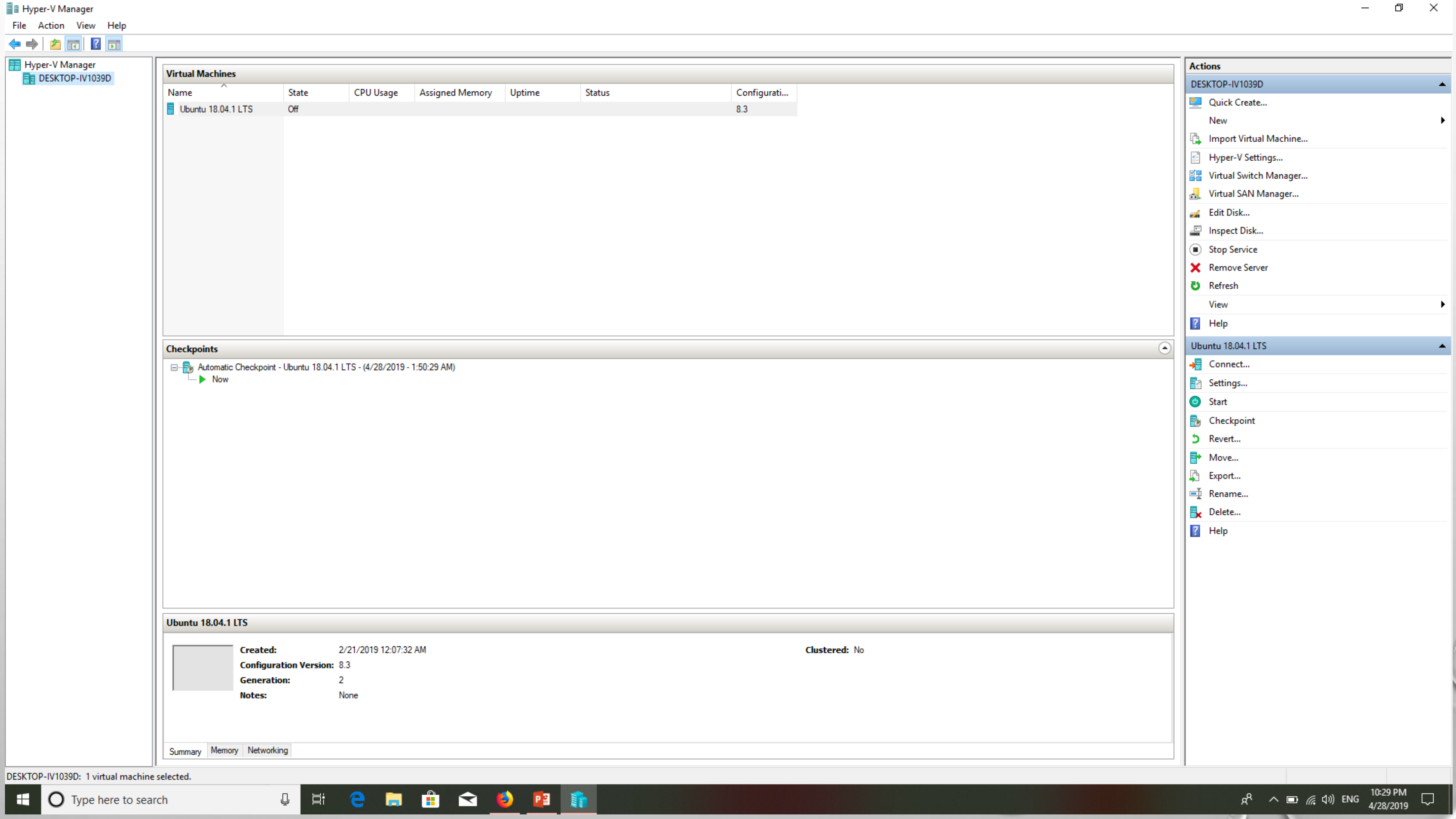
IT IS NECESSARY TO ANALYZE SECURITY POLICY OF YOUR COMPUTER:

- ✓ TO REVEAL WHETHER IT IS POSSIBLE TO CREATE AN ACCOUNT WITH AN EMPTY PASSWORD;
- ✓ TO REVEAL WHETHER ANY KIND OF AUDIT IS SET.

OS LINUX

(UBUNTU VERSION)

HYPER–V MANAGER (SNAP-IN FOR VIRTUAL MACHINES MANAGEMENT, ONLY FROM WINDOWS 10 PROFESSIONAL)



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Ubuntu 18.04.1 LTS	Off					8.3

Checkpoints

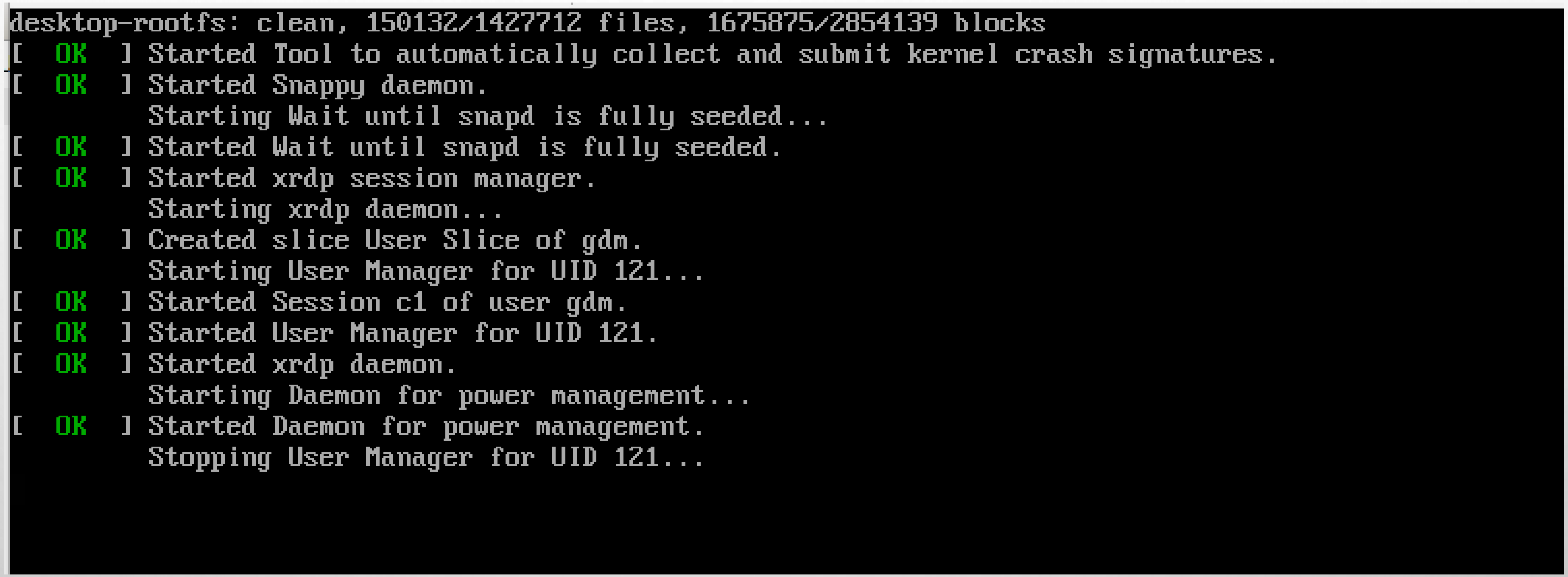
Automatic Checkpoint - Ubuntu 18.04.1 LTS - (4/28/2019 - 1:50:29 AM)
Now

Ubuntu 18.04.1 LTS

Created:	2/21/2019 12:07:32 AM	**Clustered:**	No
Configuration Version:	8.3		
Generation:	2		
Notes:	None		

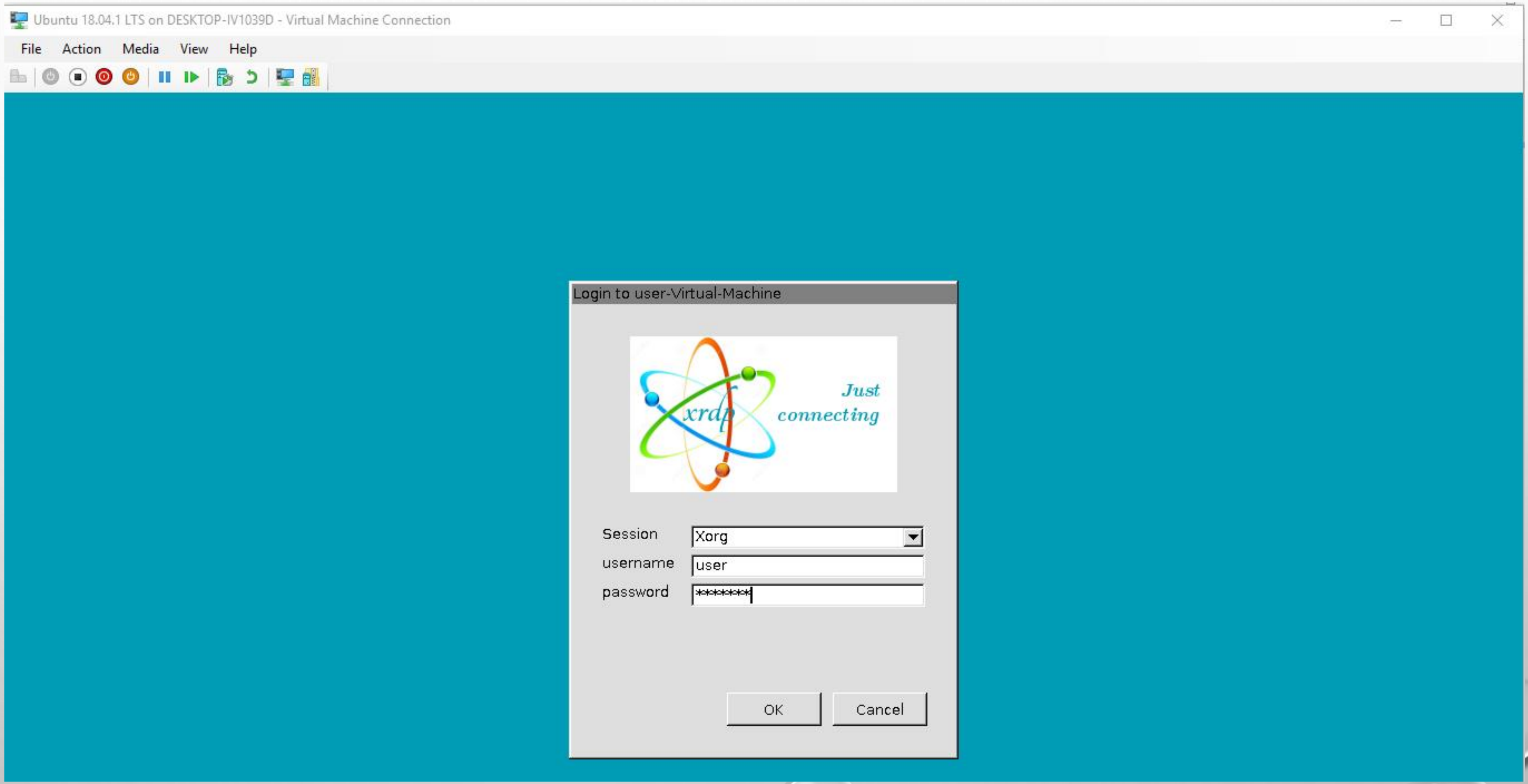
DESKTOP-IV1039D: 1 virtual machine selected.

LINUX LOADING



```
desktop-rootfs: clean, 150132/1427712 files, 1675875/2854139 blocks
[  OK  ] Started Tool to automatically collect and submit kernel crash signatures.
[  OK  ] Started Snappy daemon.
         Starting Wait until snapd is fully seeded...
[  OK  ] Started Wait until snapd is fully seeded.
[  OK  ] Started xrdp session manager.
         Starting xrdp daemon...
[  OK  ] Created slice User Slice of gdm.
         Starting User Manager for UID 121...
[  OK  ] Started Session c1 of user gdm.
[  OK  ] Started User Manager for UID 121.
[  OK  ] Started xrdp daemon.
         Starting Daemon for power management...
[  OK  ] Started Daemon for power management.
         Stopping User Manager for UID 121...
```

LOGIN IN THE VIRTUAL MACHINE:
USERNAME: user
PASSWORD: rtf-123



Ubuntu 18.04.1 LTS on DESKTOP-IV1039D - Virtual Machine Connection

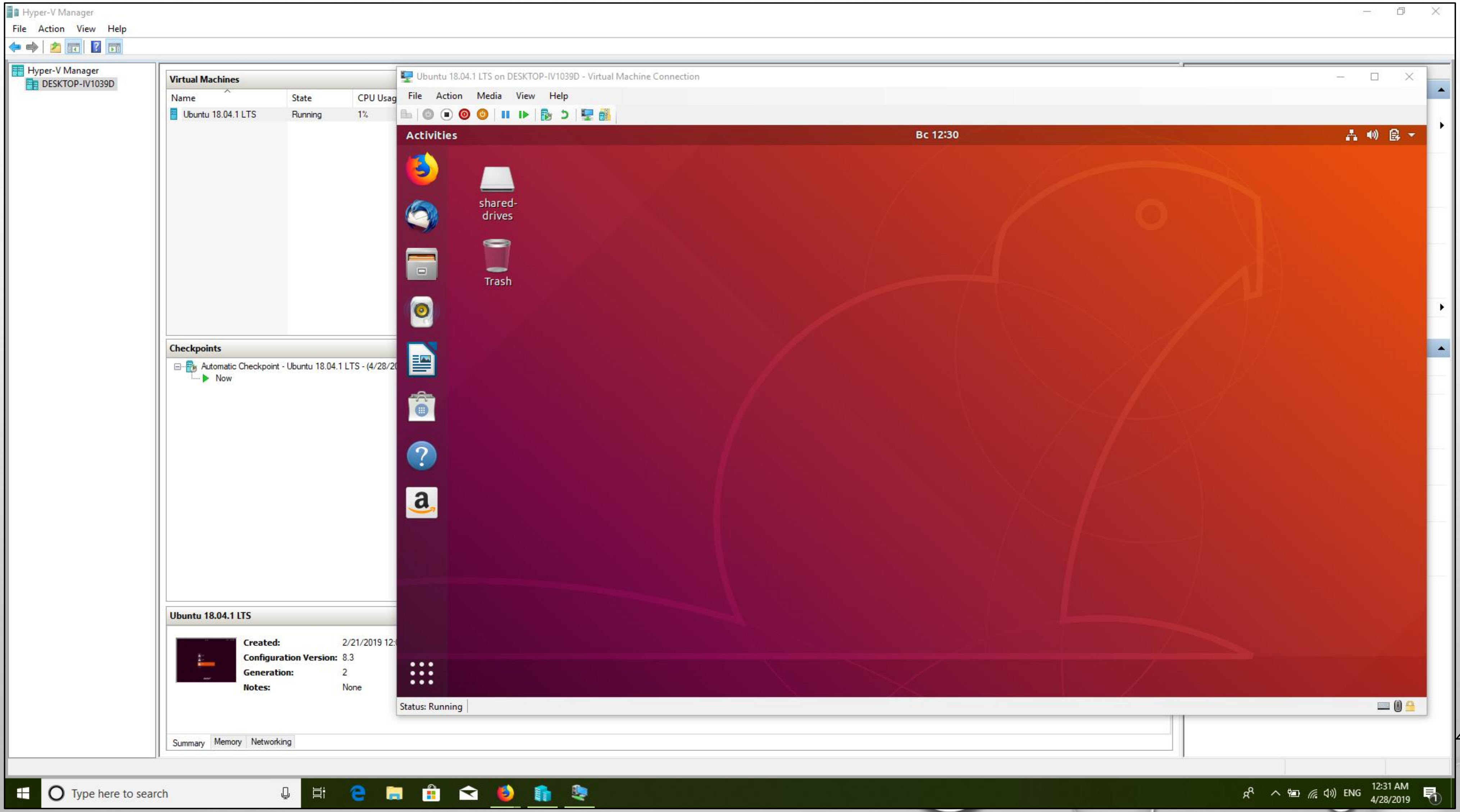
Login to user-Virtual-Machine

Session: Xorg

username: user

password: *******

FIRST SCREEN (GNOME DESKTOP)



Name	State	CPU Usag
Ubuntu 18.04.1 LTS	Running	1%

Automatic Checkpoint - Ubuntu 18.04.1 LTS - (4/28/2

Now

Ubuntu 18.04.1 LTS

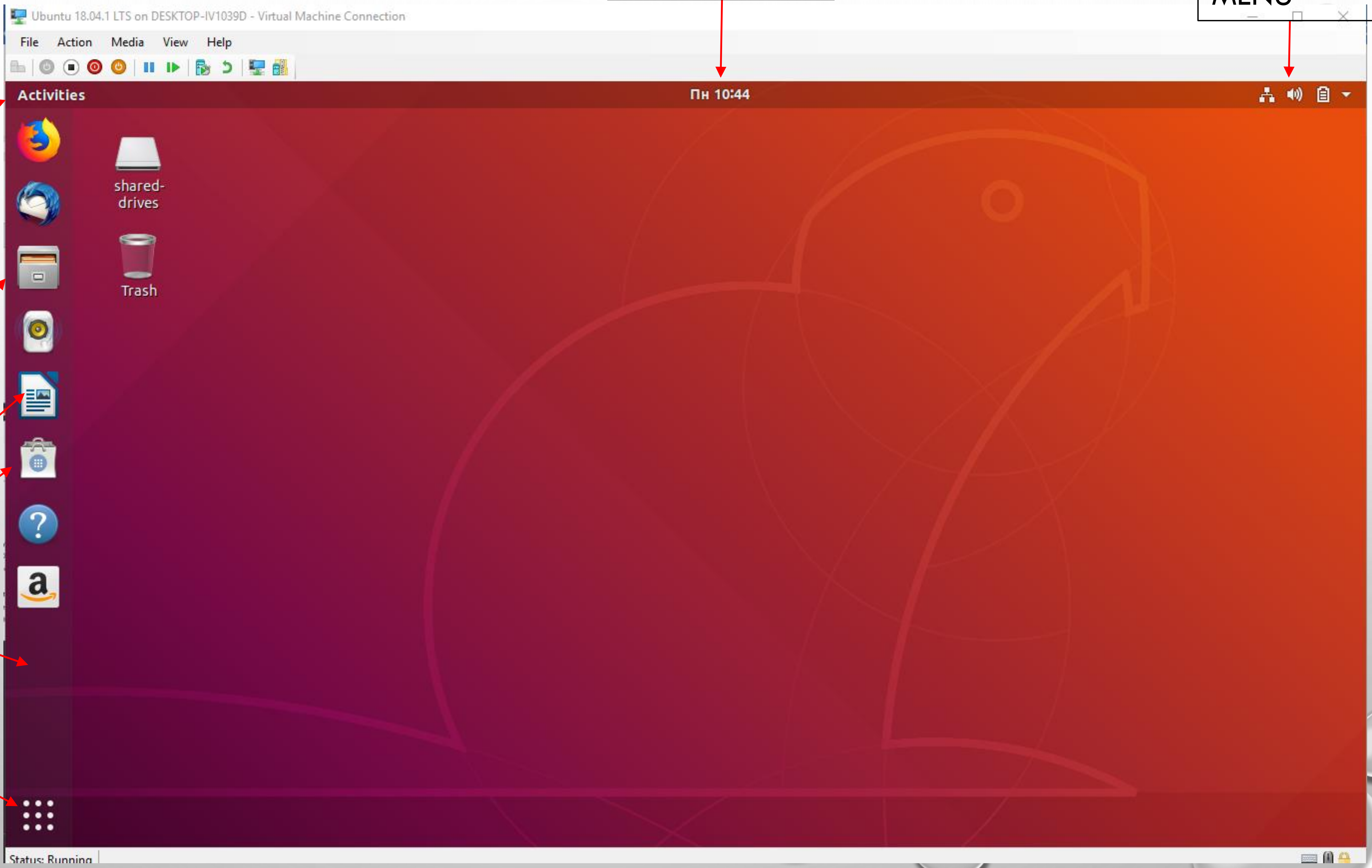
Created: 2/21/2019 12:

Configuration Version: 8.3

Generation: 2

Notes: None

Status: Running



DATE & TIME

SYSTEM MENU

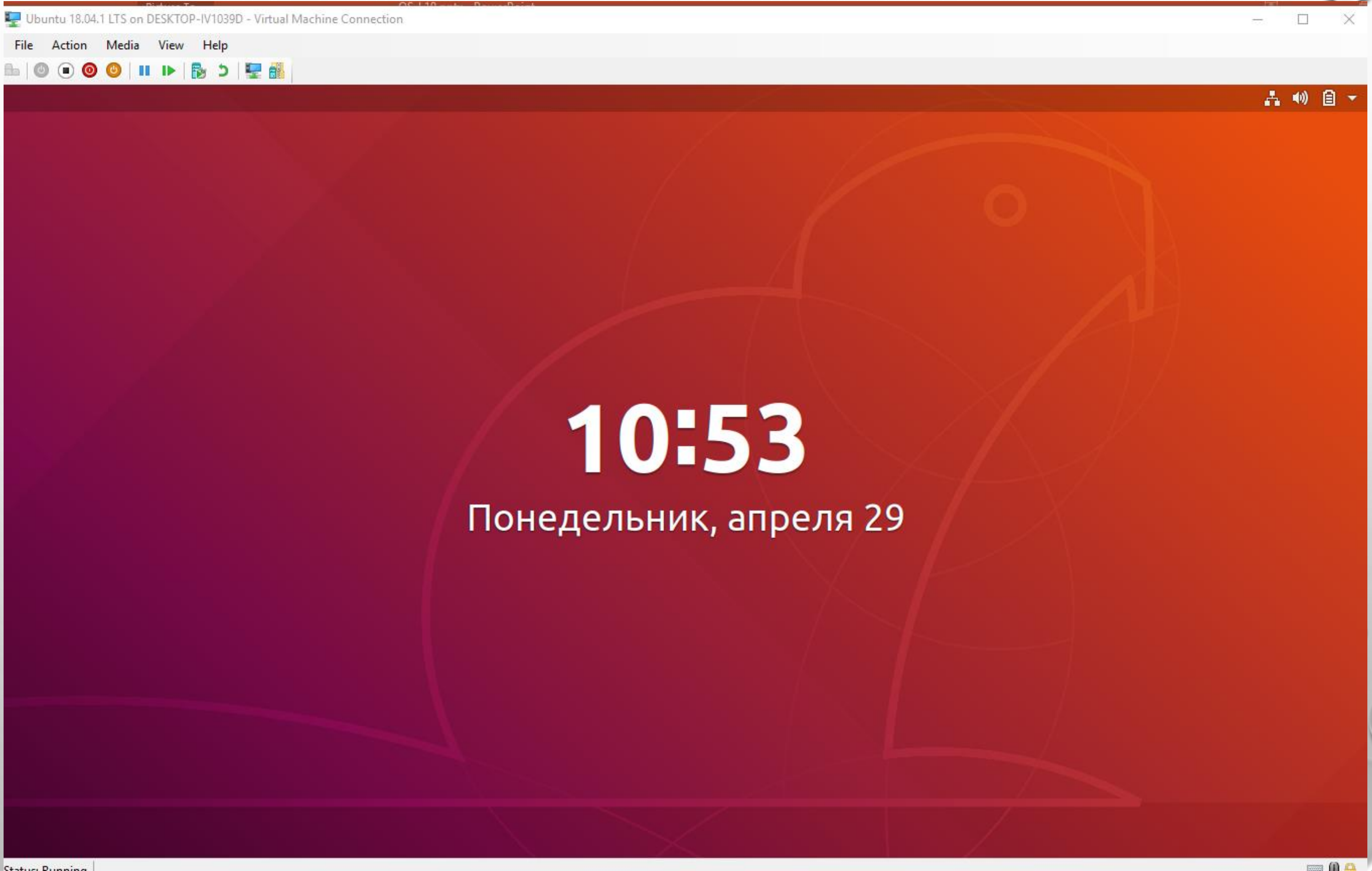
ACTIVITIES

APPLICATIONS

DASH

ALL APPLICATIONS

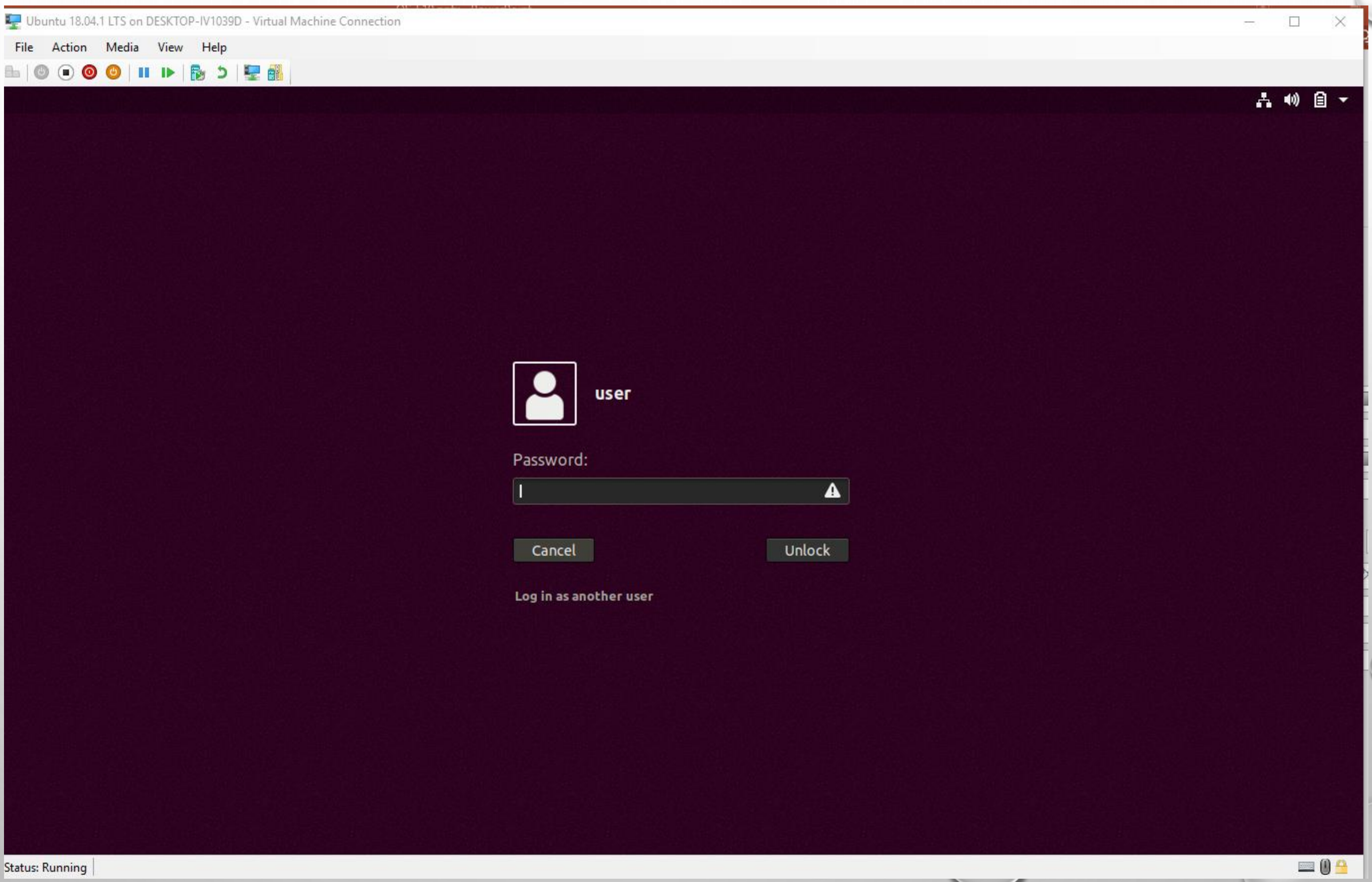
LOCK SCREEN


Ubuntu 18.04.1 LTS on DESKTOP-IV1039D - Virtual Machine Connection
File
Action
Media
View
Help

10:53

Понедельник, апреля 29

UNLOCK



Ubuntu 18.04.1 LTS on DESKTOP-IV1039D - Virtual Machine Connection

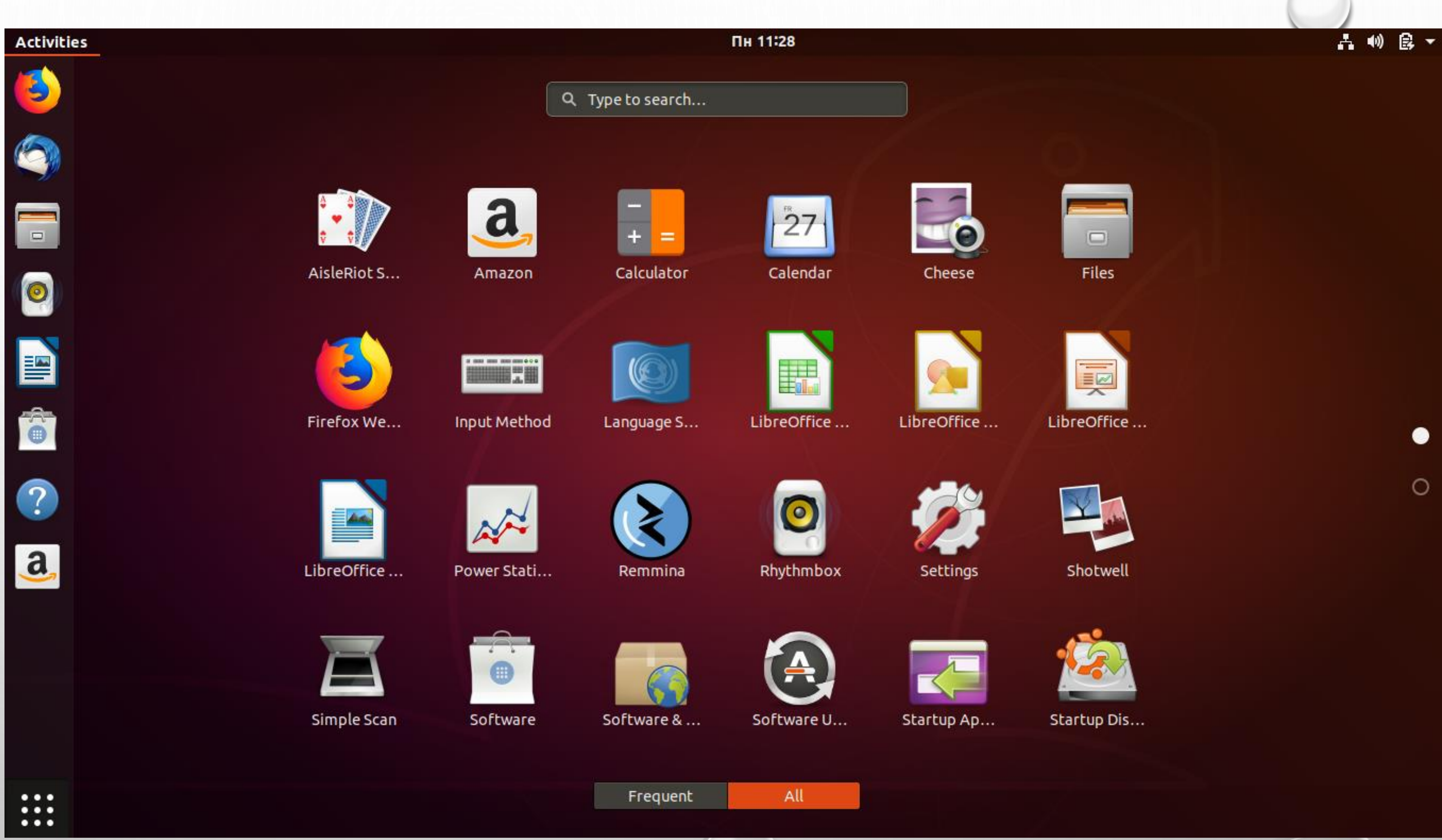
user

Password:

Status: Running

ACTIVITIES BUTTON

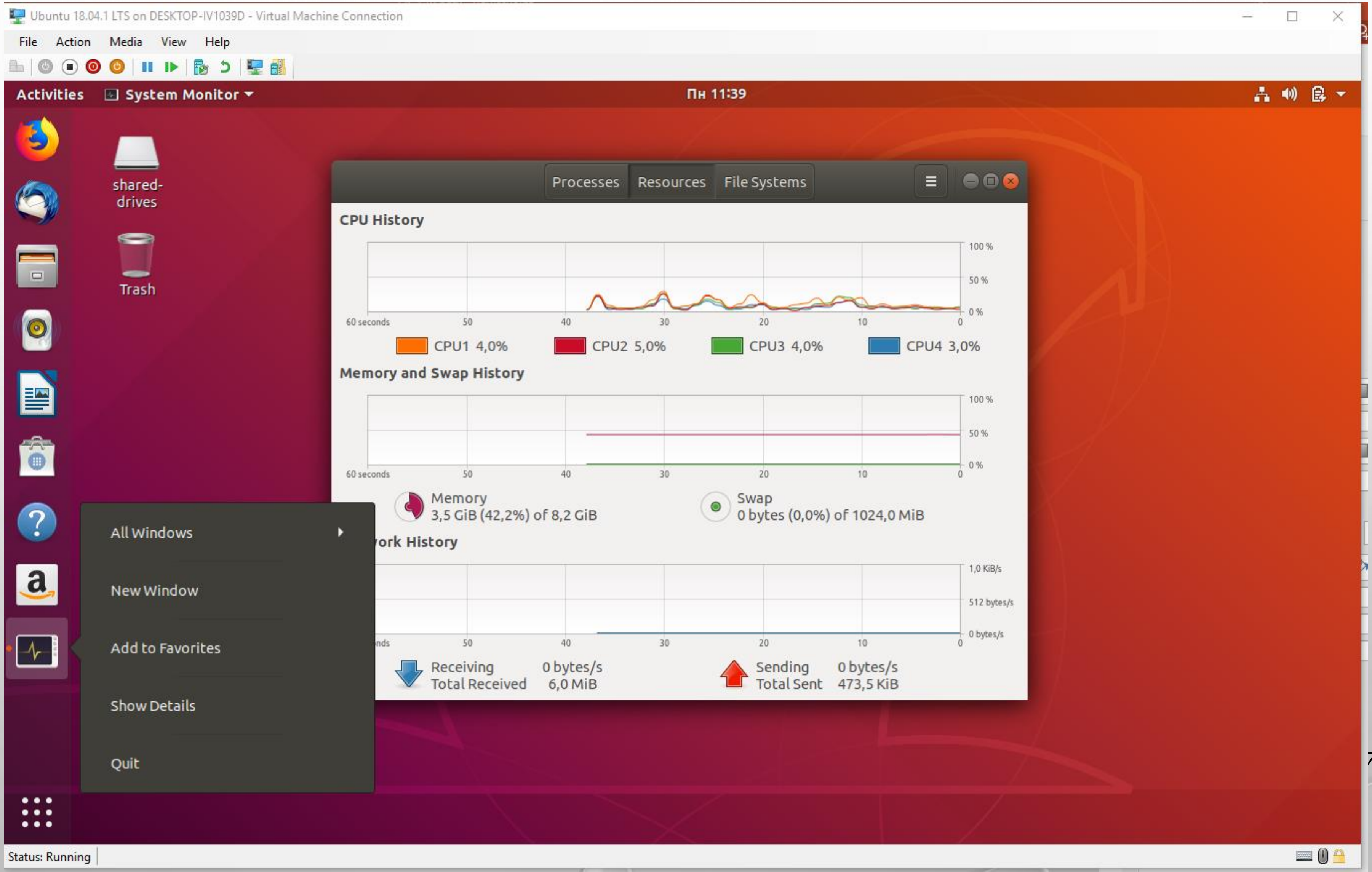
- TO ACCESS YOUR WINDOWS AND APPLICATIONS, CLICK THE ACTIVITIES BUTTON, OR JUST MOVE YOUR MOUSE POINTER TO THE TOP-LEFT HOT CORNER.
- YOU CAN ALSO PRESS THE SUPER KEY ON YOUR KEYBOARD. YOU CAN SEE YOUR WINDOWS AND APPLICATIONS IN THE OVERVIEW.
- YOU CAN ALSO JUST START TYPING TO SEARCH YOUR APPLICATIONS, FILES, FOLDERS, AND THE WEB.



THE DASH

- ➢ ON THE LEFT OF THE OVERVIEW, YOU WILL FIND **THE DASH**. THE DASH SHOWS YOU YOUR FAVORITE AND RUNNING APPLICATIONS.
- ➢ CLICK ANY ICON IN THE DASH TO OPEN THAT APPLICATION; IF THE APPLICATION IS ALREADY RUNNING, IT WILL BE HIGHLIGHTED. CLICKING ITS ICON WILL BRING UP THE MOST RECENTLY USED WINDOW. YOU CAN ALSO DRAG THE ICON TO THE OVERVIEW, OR ONTO ANY WORKSPACE ON THE RIGHT.
- ➢ RIGHT-CLICKING THE ICON DISPLAYS A MENU THAT ALLOWS YOU TO PICK ANY WINDOW IN A RUNNING APPLICATION, OR TO OPEN A NEW WINDOW. YOU CAN ALSO CLICK THE ICON WHILE HOLDING DOWN CTRL TO OPEN A NEW WINDOW.
- ➢ WHEN YOU ENTER THE OVERVIEW, YOU WILL INITIALLY BE IN THE WINDOWS OVERVIEW. THIS SHOWS YOU LIVE THUMBNAILS OF ALL THE WINDOWS ON THE CURRENT WORKSPACE.
- ➢ CLICK THE GRID BUTTON AT THE BOTTOM OF THE DASH TO DISPLAY THE APPLICATIONS OVERVIEW. THIS SHOWS YOU ALL THE APPLICATIONS INSTALLED ON YOUR COMPUTER.

RUNNING APPLICATION “SYSTEM MONITOR”



Ubuntu 18.04.1 LTS on DESKTOP-IV1039D - Virtual Machine Connection

CPU History

🟧 CPU1 4,0%   🟥 CPU2 5,0%   🟩 CPU3 4,0%   🟦 CPU4 3,0%

Memory and Swap History

Memory
3,5 GiB (42,2%) of 8,2 GiB

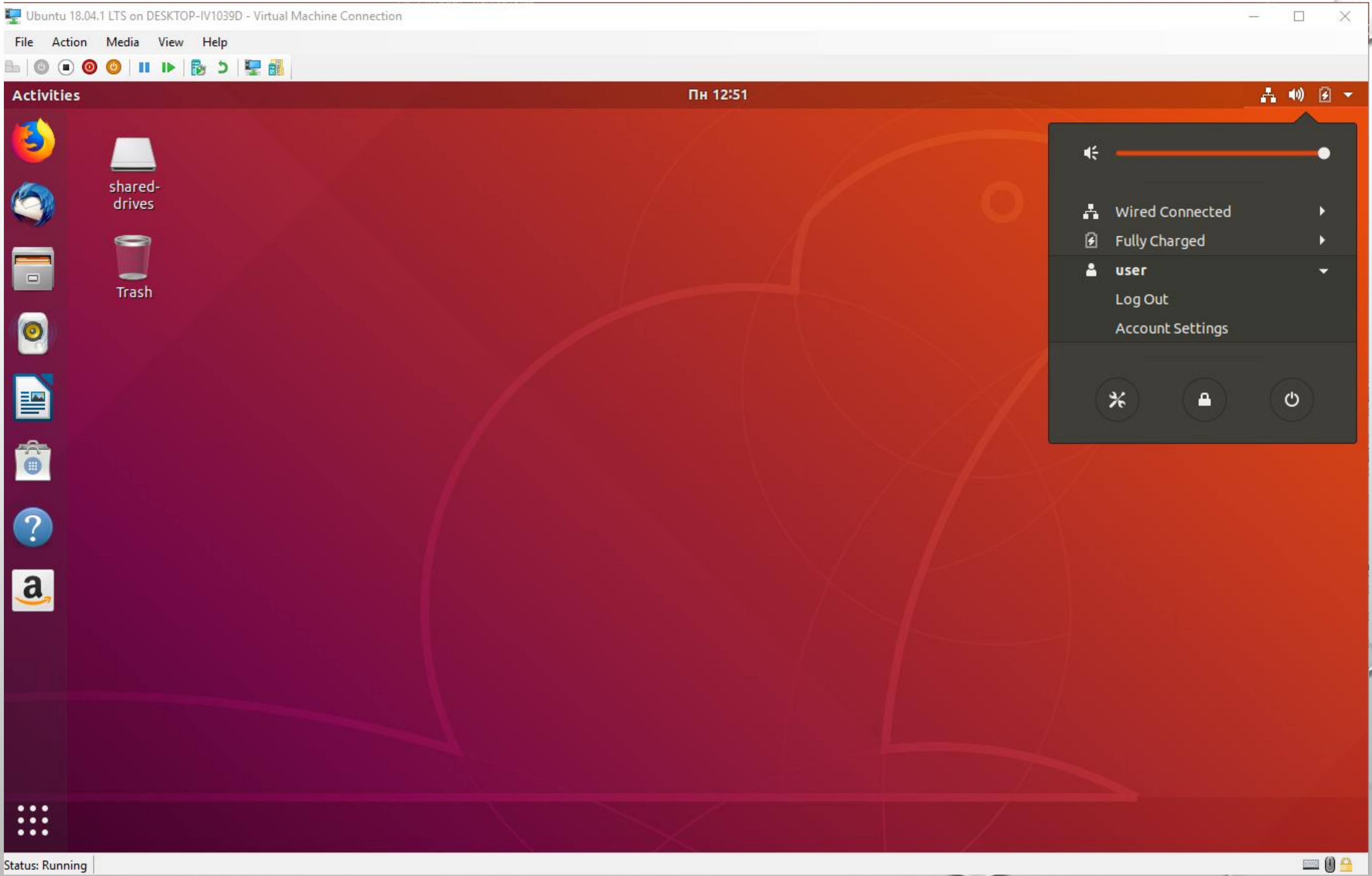
Swap
0 bytes (0,0%) of 1024,0 MiB

ork History

Receiving 0 bytes/s
Total Received 6,0 MiB

Sending 0 bytes/s
Total Sent 473,5 KiB

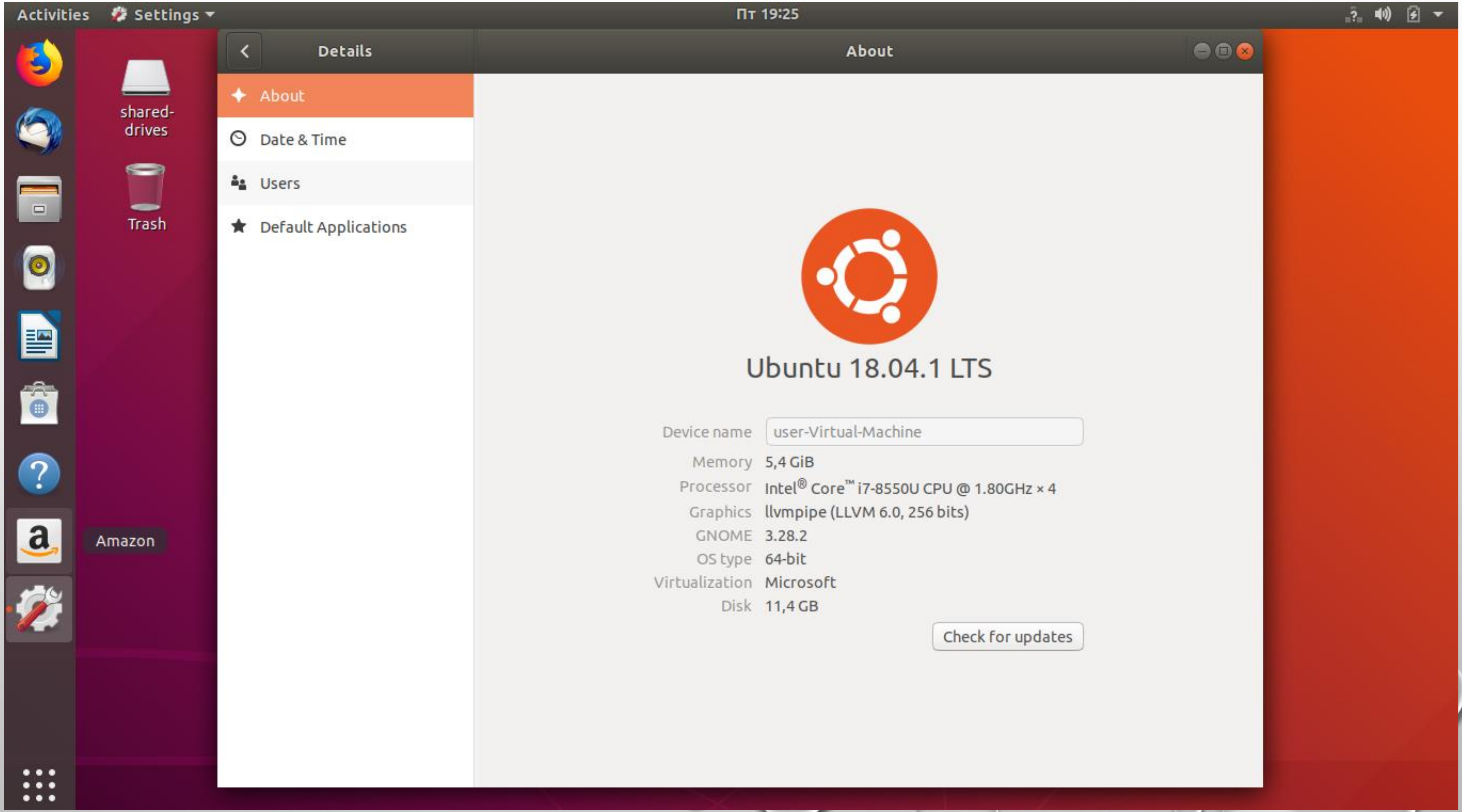
SYSTEM MENU


Ubuntu 18.04.1 LTS on DESKTOP-IV1039D - Virtual Machine Connection
File
Action
Media
View
Help
Activities
Пн 12:51
shared-drives
Trash
Wired Connected
Fully Charged
user
Log Out
Account Settings
Status: Running

SYSTEM MENU

- CLICK THE SYSTEM MENU IN THE TOP-RIGHT CORNER TO MANAGE YOUR SYSTEM SETTINGS AND YOUR COMPUTER.
- WHEN YOU LEAVE YOUR COMPUTER, YOU CAN LOCK YOUR SCREEN TO PREVENT OTHER PEOPLE FROM USING IT.
- YOU CAN ALSO QUICKLY SWITCH USERS WITHOUT LOGGING OUT COMPLETELY TO GIVE SOMEBODY ELSE ACCESS TO THE COMPUTER, OR YOU CAN SUSPEND OR POWER OFF THE COMPUTER FROM THE MENU.
- IF YOU HAVE A SCREEN THAT SUPPORTS VERTICAL OR HORIZONTAL ROTATION, YOU CAN QUICKLY ROTATE THE SCREEN FROM THE SYSTEM MENU. IF YOUR SCREEN DOES NOT SUPPORT ROTATION, YOU WILL NOT SEE THE BUTTON.

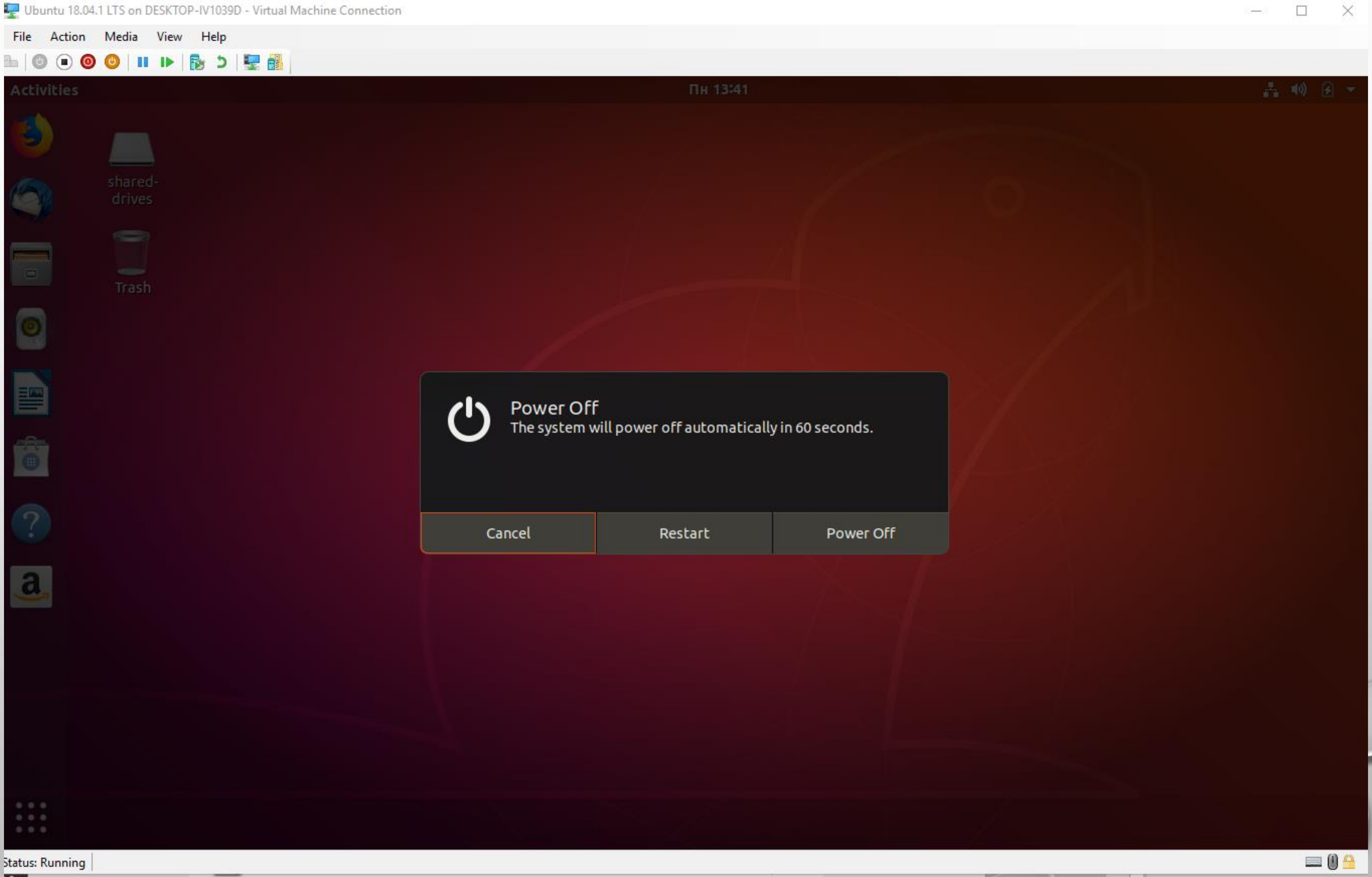
SYSTEM MENU\ABOUT



Ubuntu 18.04.1 LTS

Device name: user-Virtual-Machine
Memory: 5,4 GiB
Processor: Intel® Core™ i7-8550U CPU @ 1.80GHz × 4
Graphics: llvmpipe (LLVM 6.0, 256 bits)
GNOME: 3.28.2
OS type: 64-bit
Virtualization: Microsoft
Disk: 11,4 GB

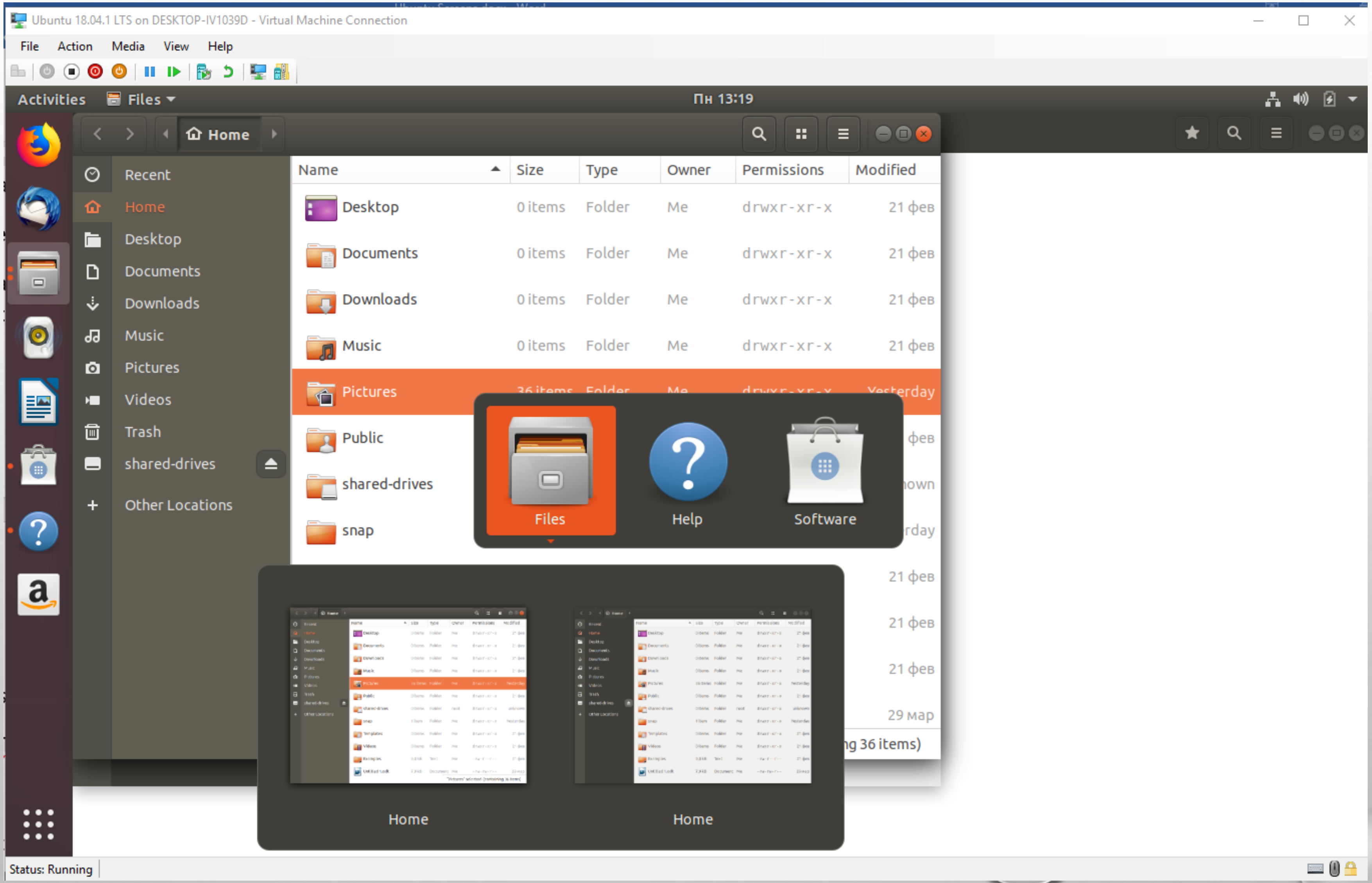
SWITCHING OFF



Power Off

The system will power off automatically in 60 seconds.

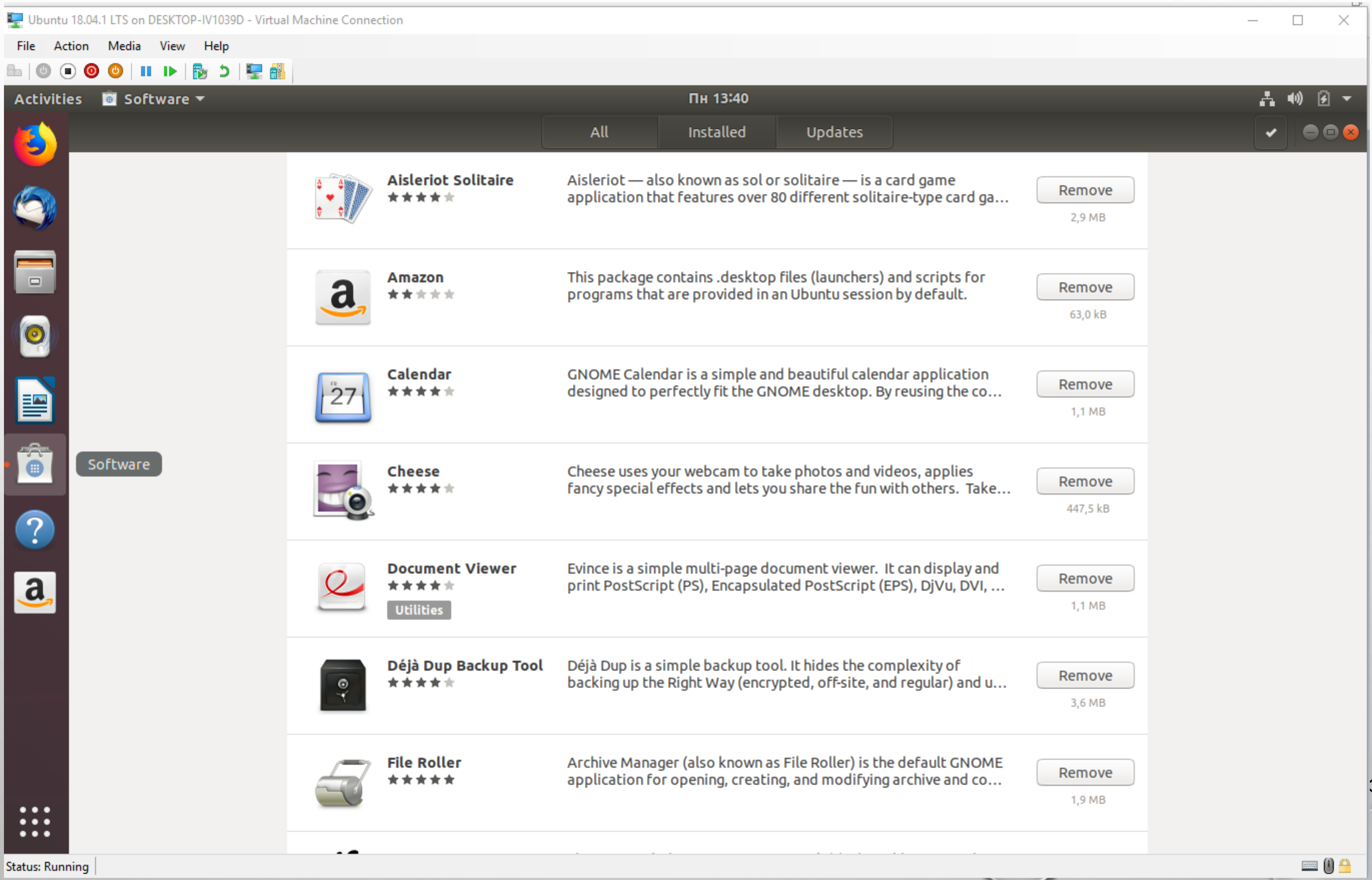
TO SWITCH BETWEEN THE WINDOWS: “SUPER”+TAB



Name	Size	Type	Owner	Permissions	Modified
Desktop	0 items	Folder	Me	drwxr-xr-x	21 фев
Documents	0 items	Folder	Me	drwxr-xr-x	21 фев
Downloads	0 items	Folder	Me	drwxr-xr-x	21 фев
Music	0 items	Folder	Me	drwxr-xr-x	21 фев
Pictures	36 items	Folder	Me	drwxr-xr-x	Yesterday
Public					фев
shared-drives					own
snap					rday
					21 фев
					21 фев
					21 фев
					29 мар

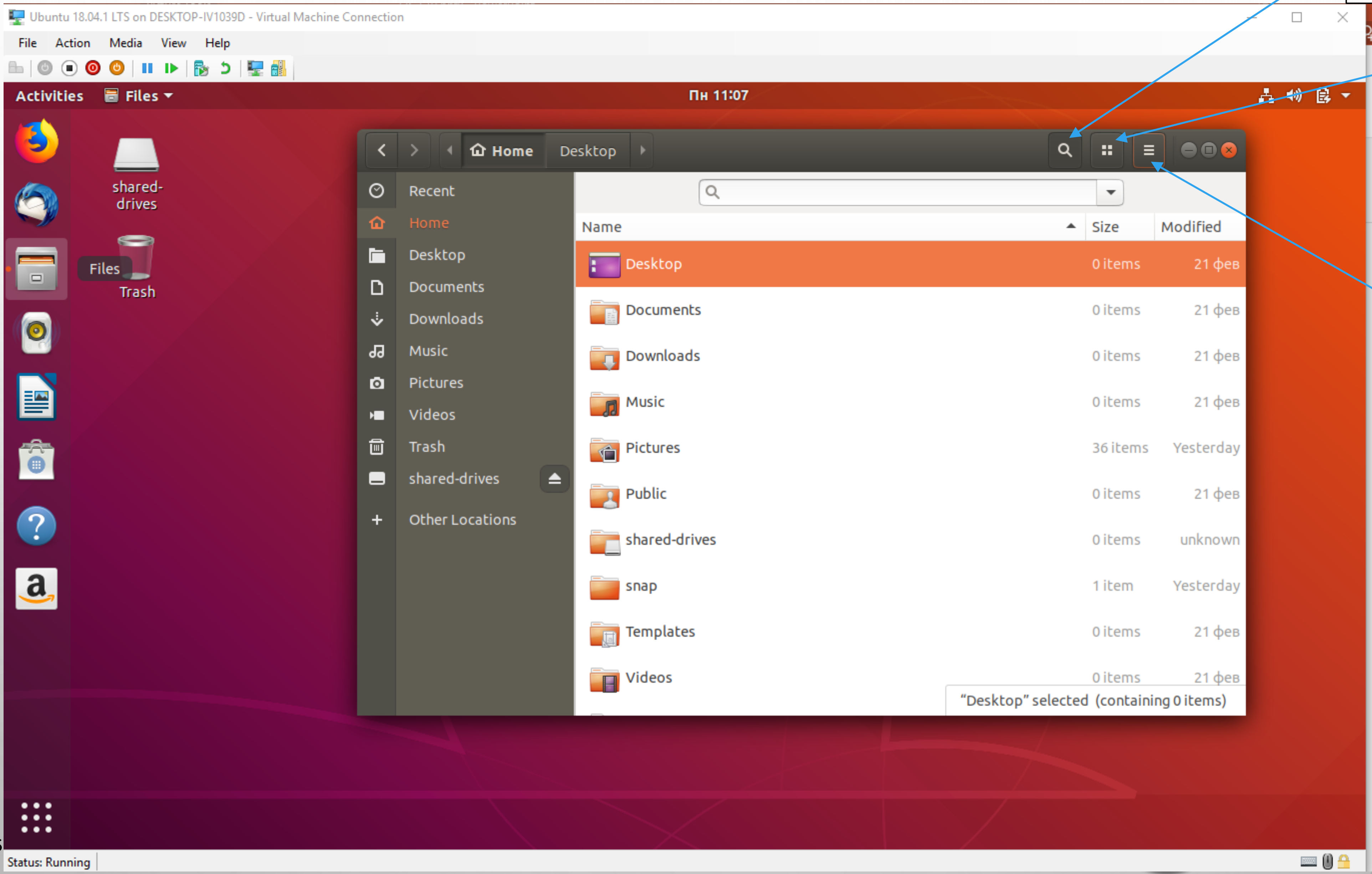
ng 36 items)

APPLICATIONS



Aisleriot Solitaire ★★★★☆	Aisleriot — also known as sol or solitaire — is a card game application that features over 80 different solitaire-type card ga…	Remove	2,9 MB
Amazon ★★☆☆☆	This package contains .desktop files (launchers) and scripts for programs that are provided in an Ubuntu session by default.	Remove	63,0 kB
Calendar ★★★★☆	GNOME Calendar is a simple and beautiful calendar application designed to perfectly fit the GNOME desktop. By reusing the co…	Remove	1,1 MB
Cheese ★★★★☆	Cheese uses your webcam to take photos and videos, applies fancy special effects and lets you share the fun with others. Take…	Remove	447,5 kB
Document Viewer ★★★★☆ Utilities	Evince is a simple multi-page document viewer. It can display and print PostScript (PS), Encapsulated PostScript (EPS), DjVu, DVI, …	Remove	1,1 MB
Déjà Dup Backup Tool ★★★★☆	Déjà Dup is a simple backup tool. It hides the complexity of backing up the Right Way (encrypted, off-site, and regular) and u…	Remove	3,6 MB
File Roller ★★★★★	Archive Manager (also known as File Roller) is the default GNOME application for opening, creating, and modifying archive and co…	Remove	1,9 MB

NAUTILUS (FILES) – A FILE MANAGER OF THE GNOME DESKTOP



Name	Size	Modified
Desktop	0 items	21 фев
Documents	0 items	21 фев
Downloads	0 items	21 фев
Music	0 items	21 фев
Pictures	36 items	Yesterday
Public	0 items	21 фев
shared-drives	0 items	unknown
snap	1 item	Yesterday
Templates	0 items	21 фев
Videos	0 items	21 фев

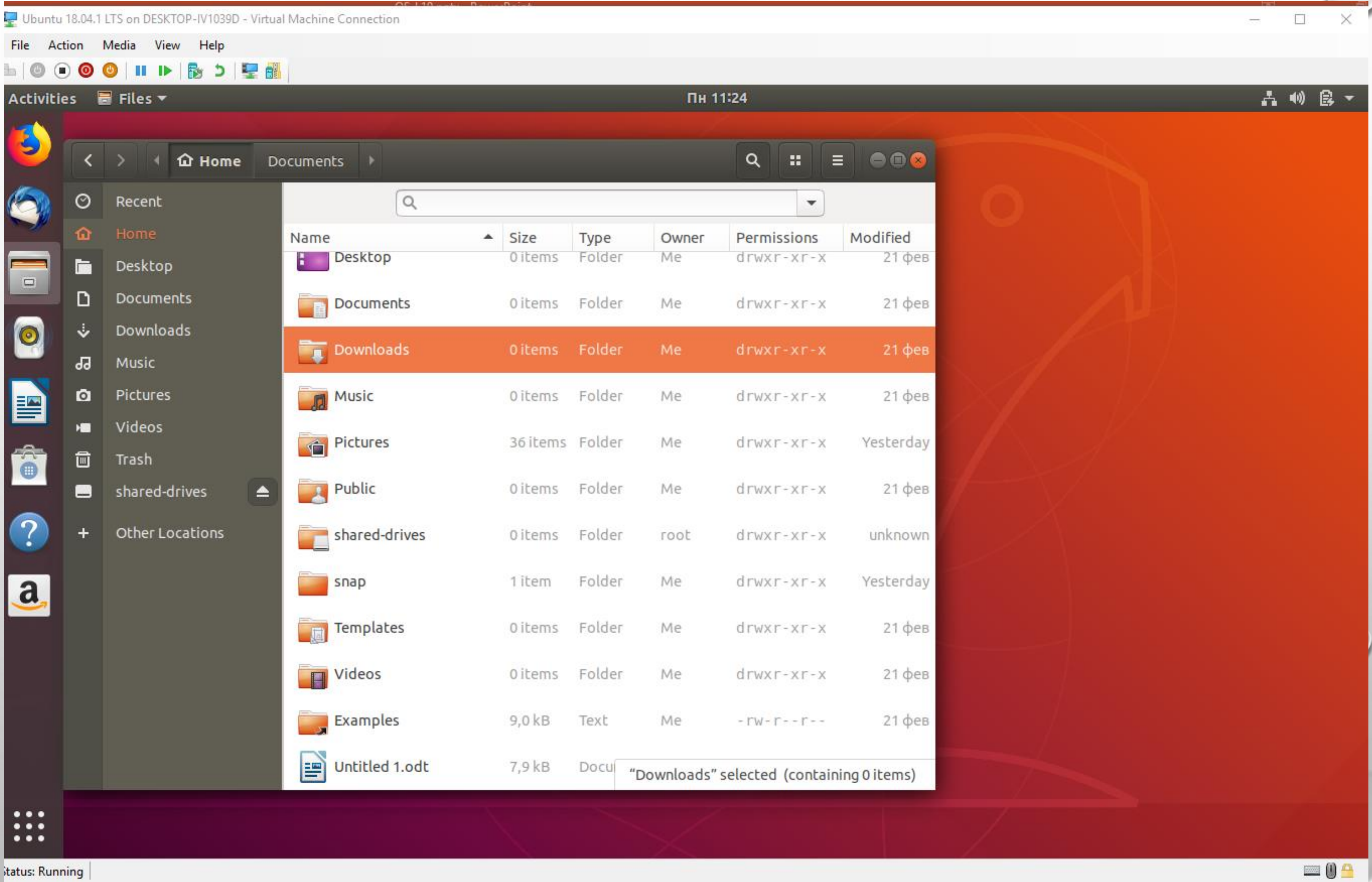
“Desktop” selected (containing 0 items)

TO SEARCH FILES

TO CHANGE LAYOUT OF FILES

TO CHANGE COLUMNS IN LAYOUT

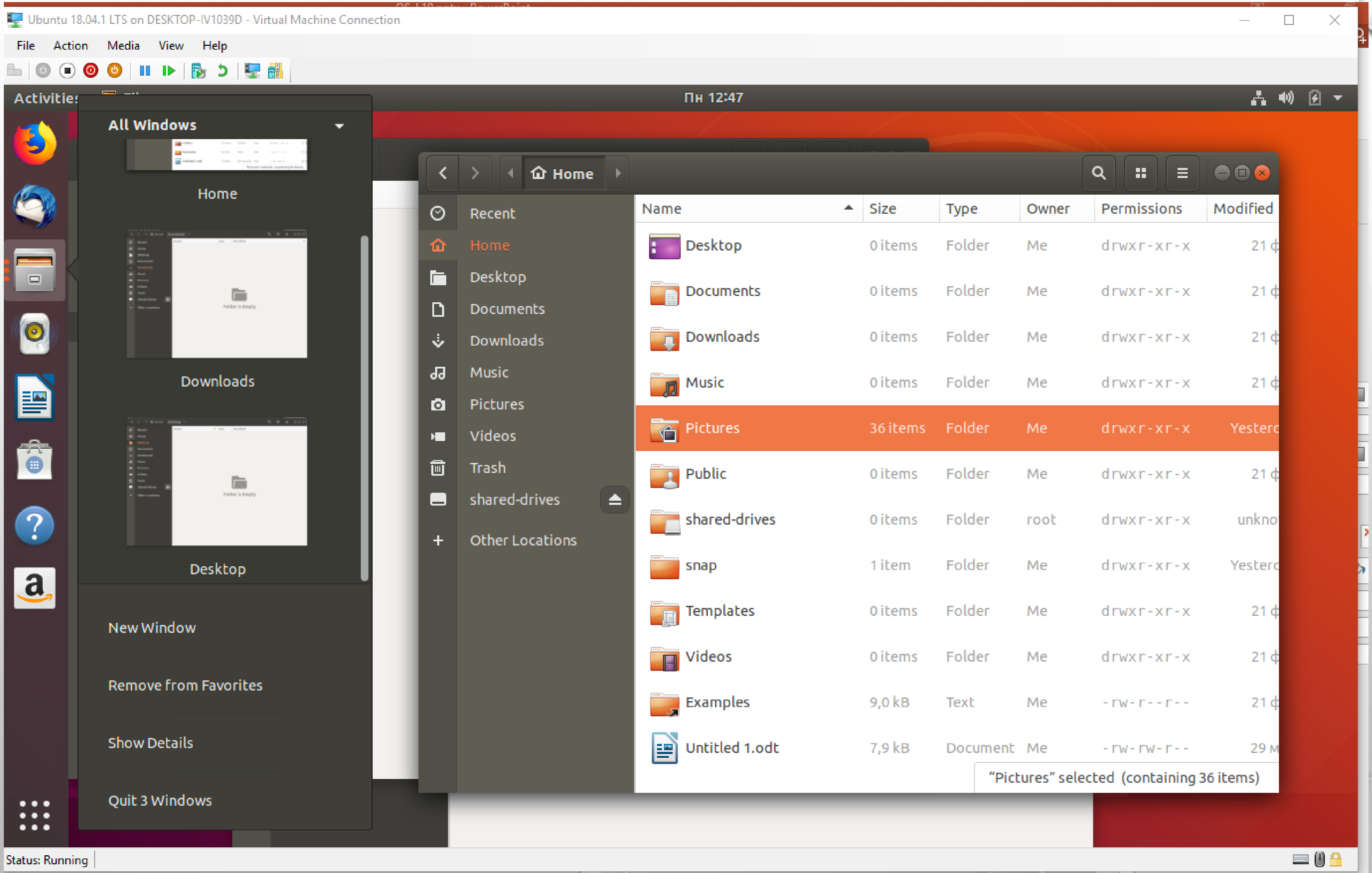
NAUTILUS: ADDITIONAL COLUMNS



Name	Size	Type	Owner	Permissions	Modified
Desktop	0 items	Folder	Me	drwxr-xr-x	21 фев
Documents	0 items	Folder	Me	drwxr-xr-x	21 фев
Downloads	0 items	Folder	Me	drwxr-xr-x	21 фев
Music	0 items	Folder	Me	drwxr-xr-x	21 фев
Pictures	36 items	Folder	Me	drwxr-xr-x	Yesterday
Public	0 items	Folder	Me	drwxr-xr-x	21 фев
shared-drives	0 items	Folder	root	drwxr-xr-x	unknown
snap	1 item	Folder	Me	drwxr-xr-x	Yesterday
Templates	0 items	Folder	Me	drwxr-xr-x	21 фев
Videos	0 items	Folder	Me	drwxr-xr-x	21 фев
Examples	9,0 kB	Text	Me	-rw-r--r--	21 фев
Untitled 1.odt	7,9 kB	Docu			

“Downloads” selected (containing 0 items)

NAUTILUS: SEVERAL WINDOWS



Name	Size	Type	Owner	Permissions	Modified
Desktop	0 items	Folder	Me	drwxr-xr-x	21 ф
Documents	0 items	Folder	Me	drwxr-xr-x	21 ф
Downloads	0 items	Folder	Me	drwxr-xr-x	21 ф
Music	0 items	Folder	Me	drwxr-xr-x	21 ф
Pictures	36 items	Folder	Me	drwxr-xr-x	Yesterd
Public	0 items	Folder	Me	drwxr-xr-x	21 ф
shared-drives	0 items	Folder	root	drwxr-xr-x	unkno
snap	1 item	Folder	Me	drwxr-xr-x	Yesterd
Templates	0 items	Folder	Me	drwxr-xr-x	21 ф
Videos	0 items	Folder	Me	drwxr-xr-x	21 ф
Examples	9,0 kB	Text	Me	-rw-r--r--	21 ф
Untitled 1.odt	7,9 kB	Document	Me	-rw-rw-r--	29 м

"Pictures" selected (containing 36 items)

Status: Running