Questions, Issues,

Concerns, Suggestions

Welcome at any time

Even Now

Sun City Computer Club

Windows SIG

September 25, 2018

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

Safe enough?

- Windows 10 October 2018 Update

  Smart Updater delay?

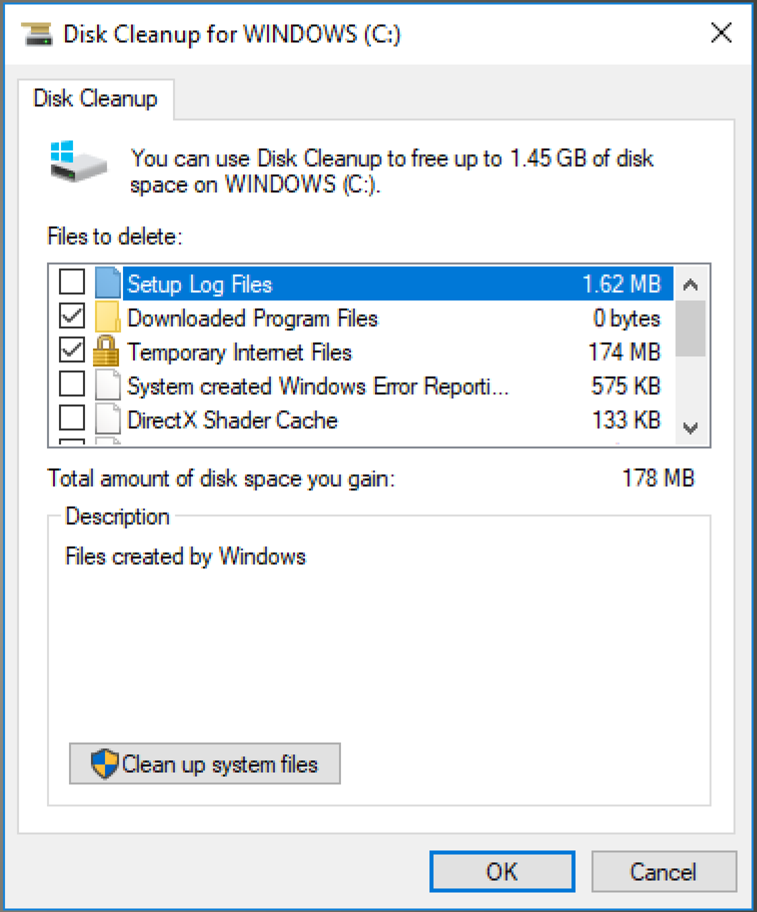
  Small disk system? 32GB or less
- Recent updates out of band

Windows News

- Empty recycle bin
- Clean temporary files
- Move photos, videos
- Remove downloads
- Disk Cleanup tool

- Storage Sense app

- Media Creation Tool
- 3-2-1 backup


Disk Cleanup for WINDOWS (C:)

Disk Cleanup

You can use Disk Cleanup to free up to 1.45 GB of disk space on WINDOWS (C:).

Files to delete:

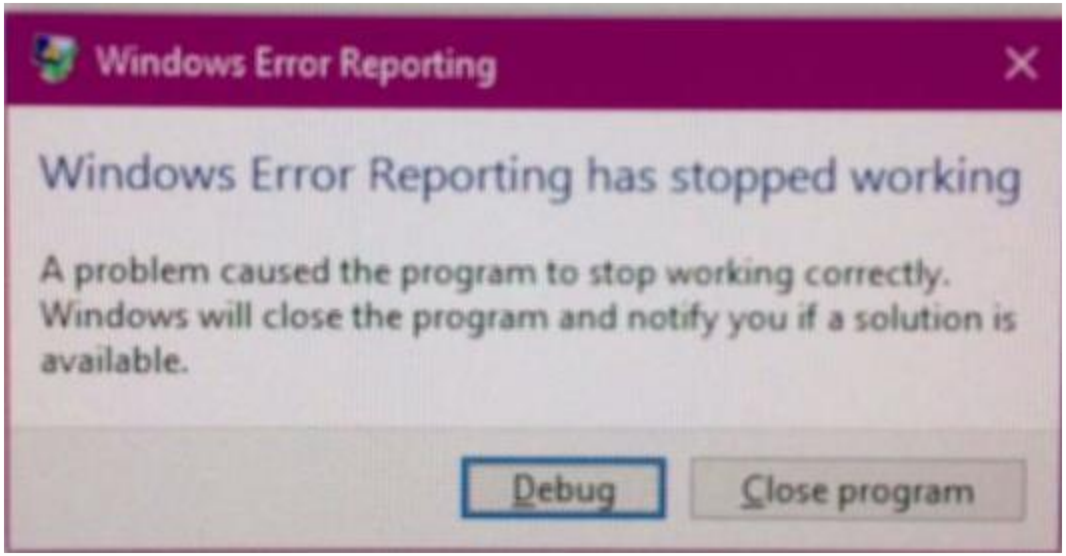
☐	Setup Log Files	1.62 MB
☑	Downloaded Program Files	0 bytes
☑	Temporary Internet Files	174 MB
☐	System created Windows Error Reporti...	575 KB
☐	DirectX Shader Cache	133 KB

Total amount of disk space you gain: 178 MB

Description

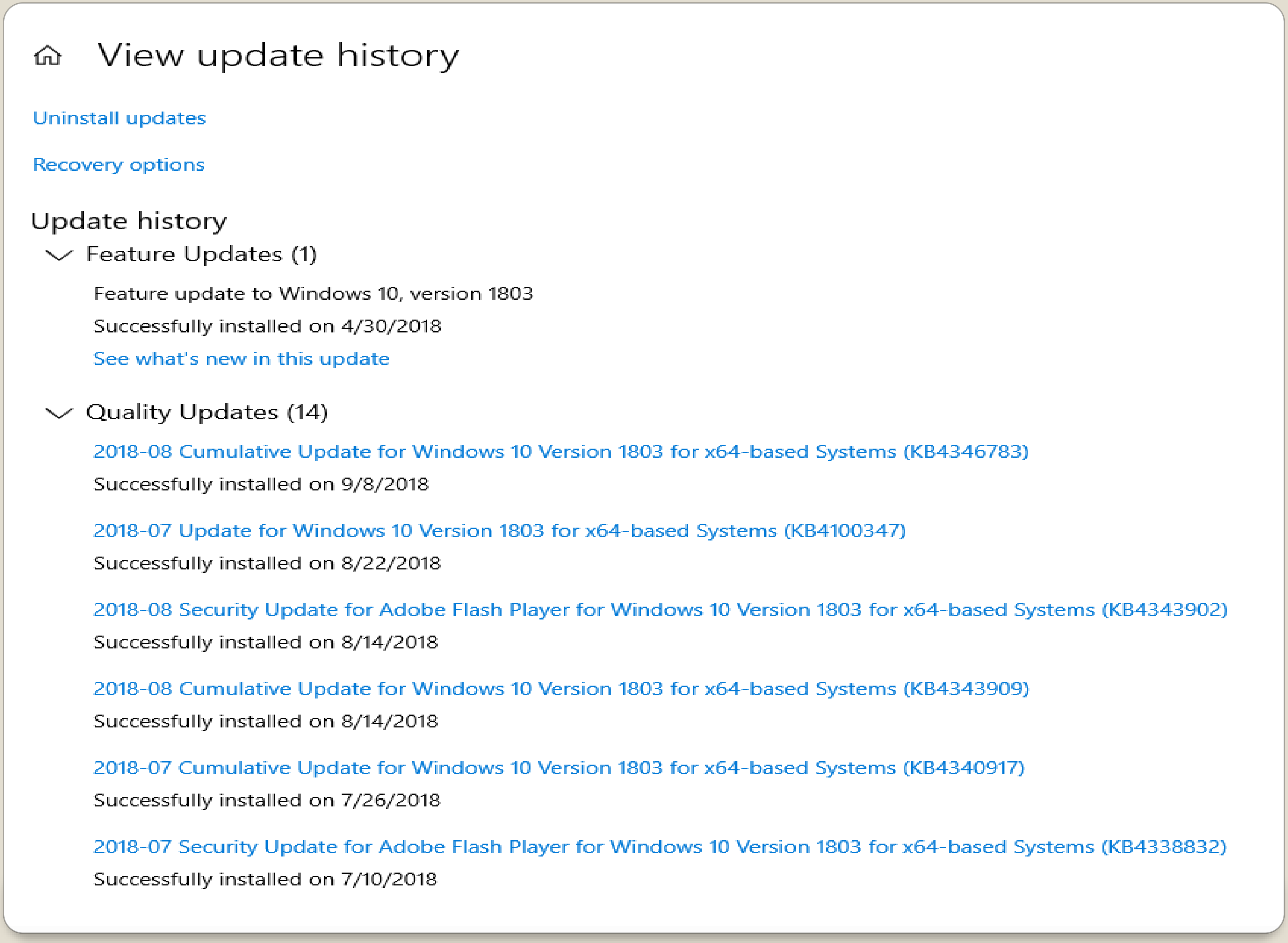
Files created by Windows

Regular regimen of system maintenance



Windows Error Reporting has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.



View update history

Uninstall updates

Recovery options

Update history

Feature Updates (1)

Feature update to Windows 10, version 1803

Successfully installed on 4/30/2018

See what's new in this update

Quality Updates (14)

2018-08 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4346783)

Successfully installed on 9/8/2018

2018-07 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347)

Successfully installed on 8/22/2018

2018-08 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4343902)

Successfully installed on 8/14/2018

2018-08 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4343909)

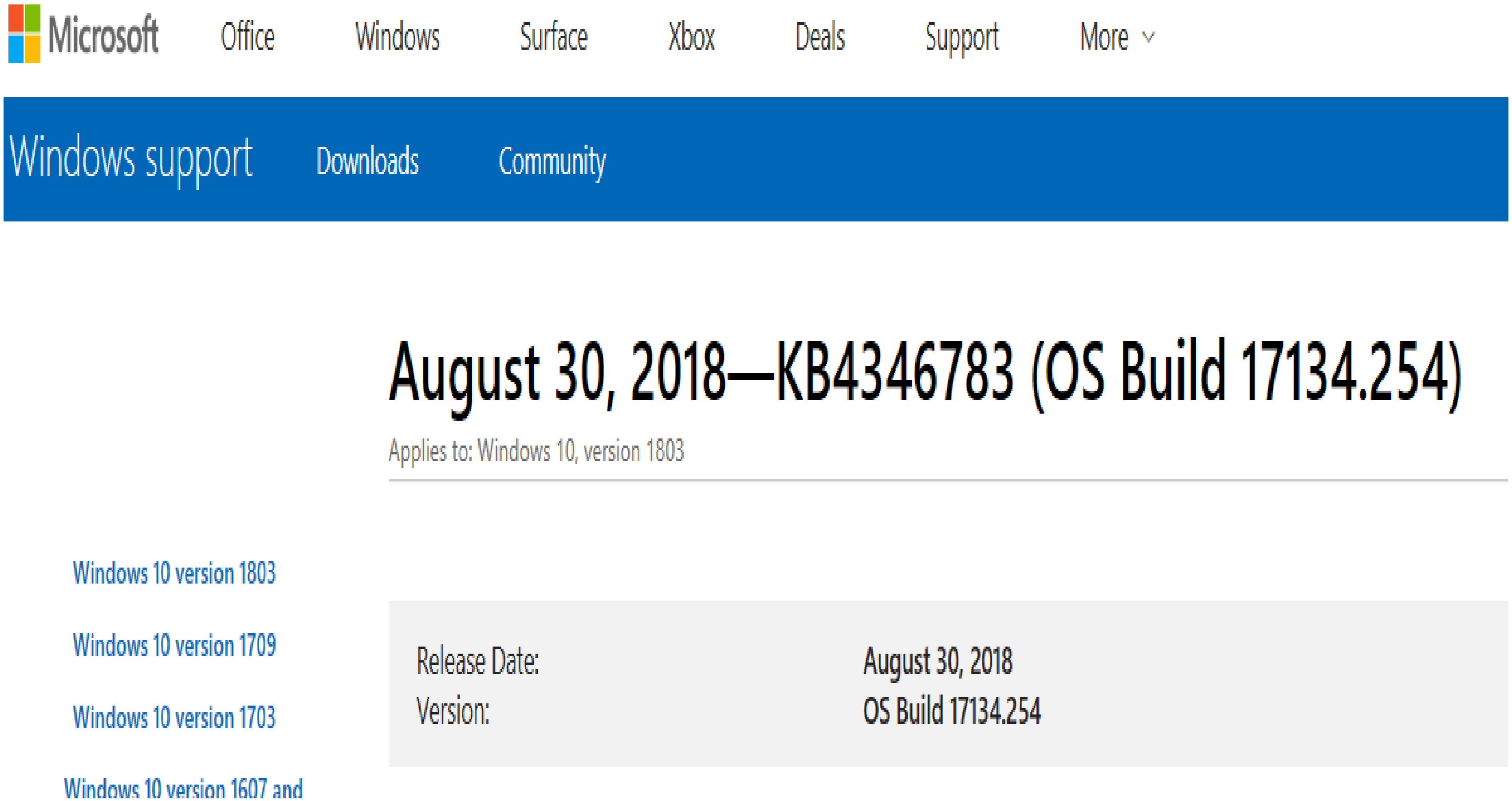
Successfully installed on 8/14/2018

2018-07 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4340917)

Successfully installed on 7/26/2018

2018-07 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4338832)

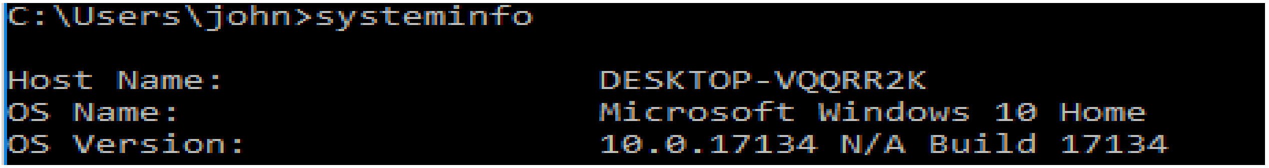
Successfully installed on 7/10/2018



August 30, 2018—KB4346783 (OS Build 17134.254)

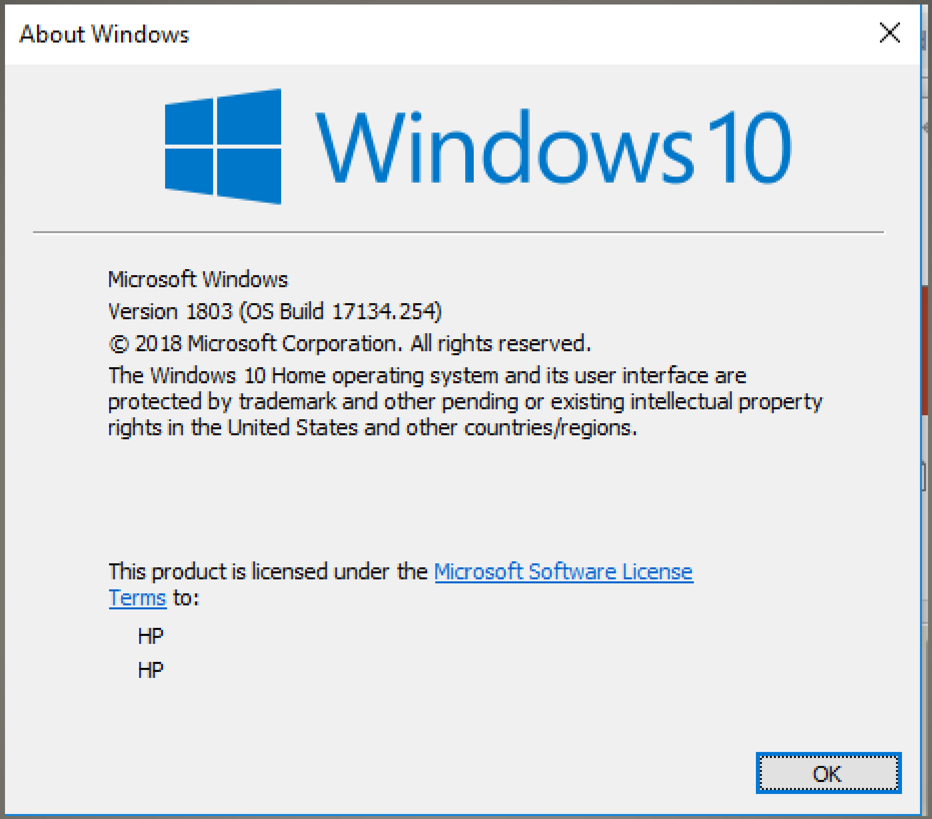
Applies to: Windows 10, version 1803

Release Date:	August 30, 2018
Version:	OS Build 17134.254



```
C:\Users\john>systeminfo

Host Name:                 DESKTOP-VQQRR2K
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.17134 N/A Build 17134
```



Microsoft Windows
Version 1803 (OS Build 17134.254)
© 2018 Microsoft Corporation. All rights reserved.
The Windows 10 Home operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

HP
HP

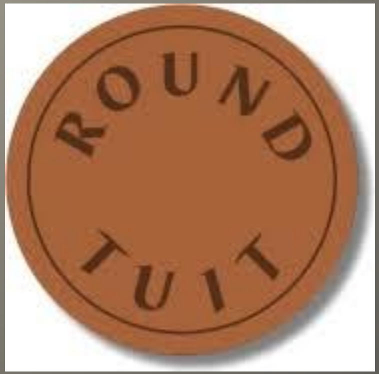
winver

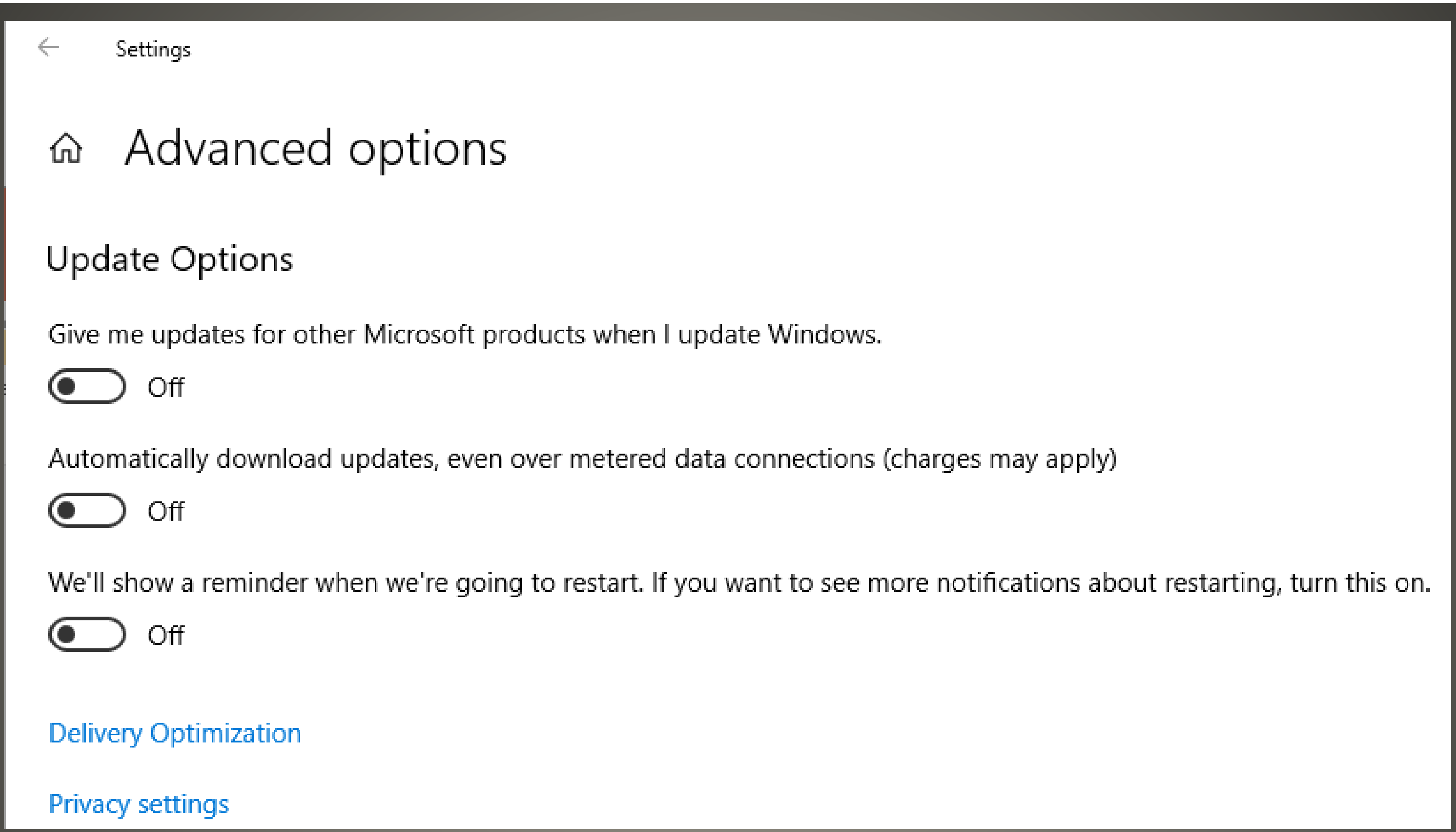
SIG News

- Switch from Gmail to Computer club’s email
- Too much cyber – message received

- Survey

1) I can’t wait to patch Windows
2) I avoid patching as long as possible
3) I patch when I get a





Settings

Advanced options

Update Options

Give me updates for other Microsoft products when I update Windows.

Off

Automatically download updates, even over metered data connections (charges may apply)

Off

We'll show a reminder when we're going to restart. If you want to see more notifications about restarting, turn this on.

Off

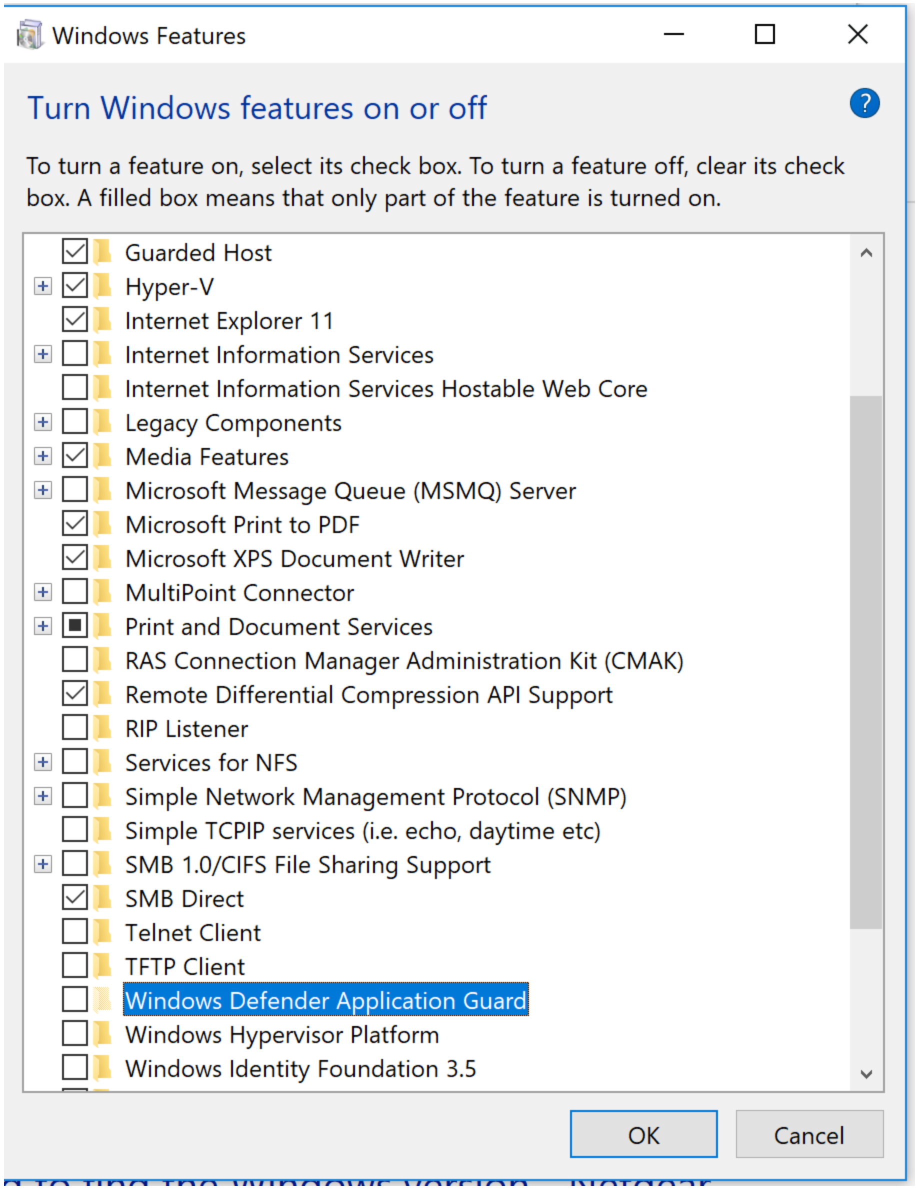
Delivery Optimization

Privacy settings

Windows Update

Windows Defender Application Guard

- Windows Pro and Enterprise
- Hypervisor support
- Hardware
- Policy Modification and Tuning (Domain)
- For Edge and Internet Explorer only
- InPrivate Desktop



Windows Features

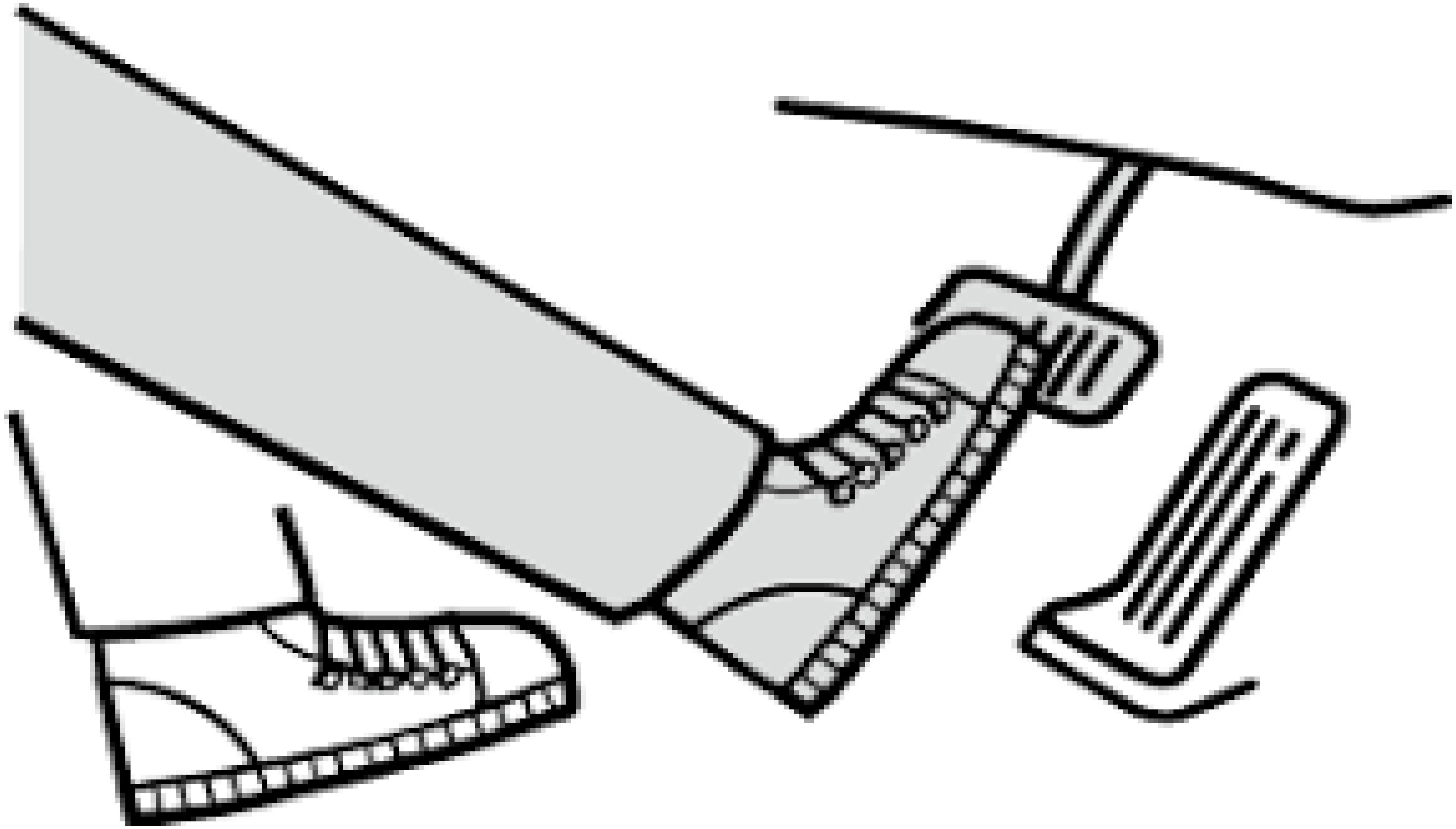
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Guarded Host
- ☑ Hyper-V
- ☑ Internet Explorer 11
- ☐ Internet Information Services
- ☐ Internet Information Services Hostable Web Core
- ☐ Legacy Components
- ☑ Media Features
- ☐ Microsoft Message Queue (MSMQ) Server
- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer
- ☐ MultiPoint Connector
- ▣ Print and Document Services
- ☐ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression API Support
- ☐ RIP Listener
- ☐ Services for NFS
- ☐ Simple Network Management Protocol (SNMP)
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ☐ SMB 1.0/CIFS File Sharing Support
- ☑ SMB Direct
- ☐ Telnet Client
- ☐ TFTP Client
- ☐ Windows Defender Application Guard
- ☐ Windows Hypervisor Platform
- ☐ Windows Identity Foundation 3.5

- Requires resources
- Takes time
- Download retries
- Malware is afraid
- Red pill
- Determine “Why?”

Sandbox, Containers, VM



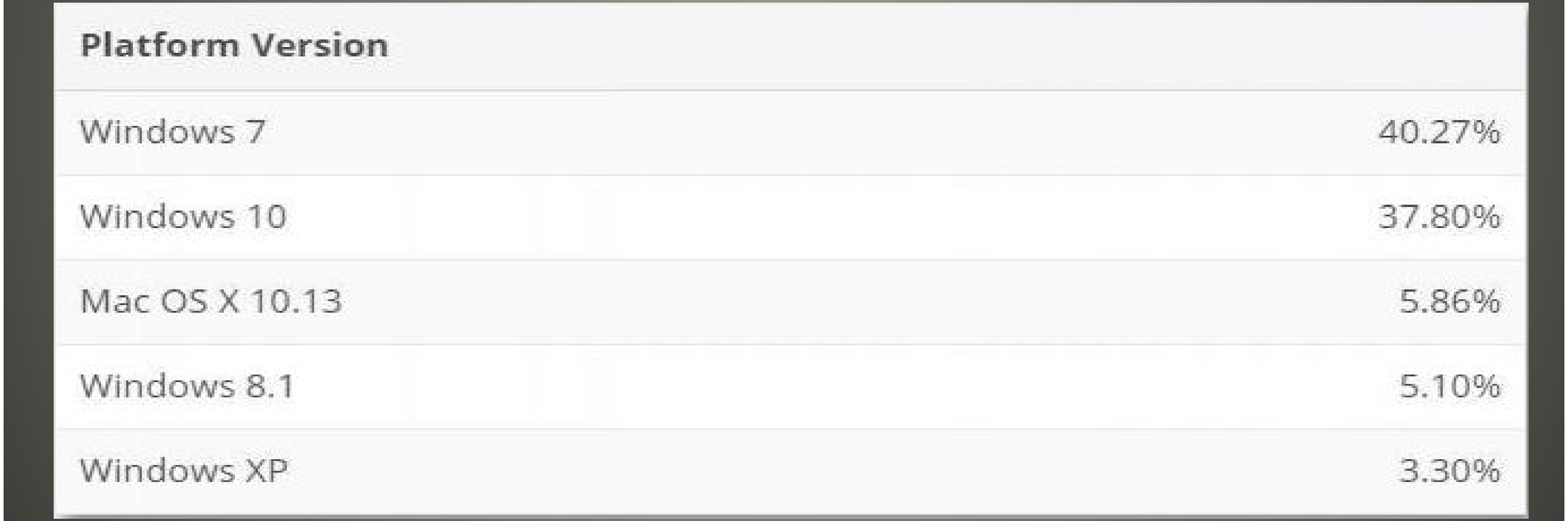
Windows 7

- Windows 7 Extended support

  Was January 2020

  Now January 2023

  Pricing to increase every year



Platform Version	
Windows 7	40.27%
Windows 10	37.80%
Mac OS X 10.13	5.86%
Windows 8.1	5.10%
Windows XP	3.30%

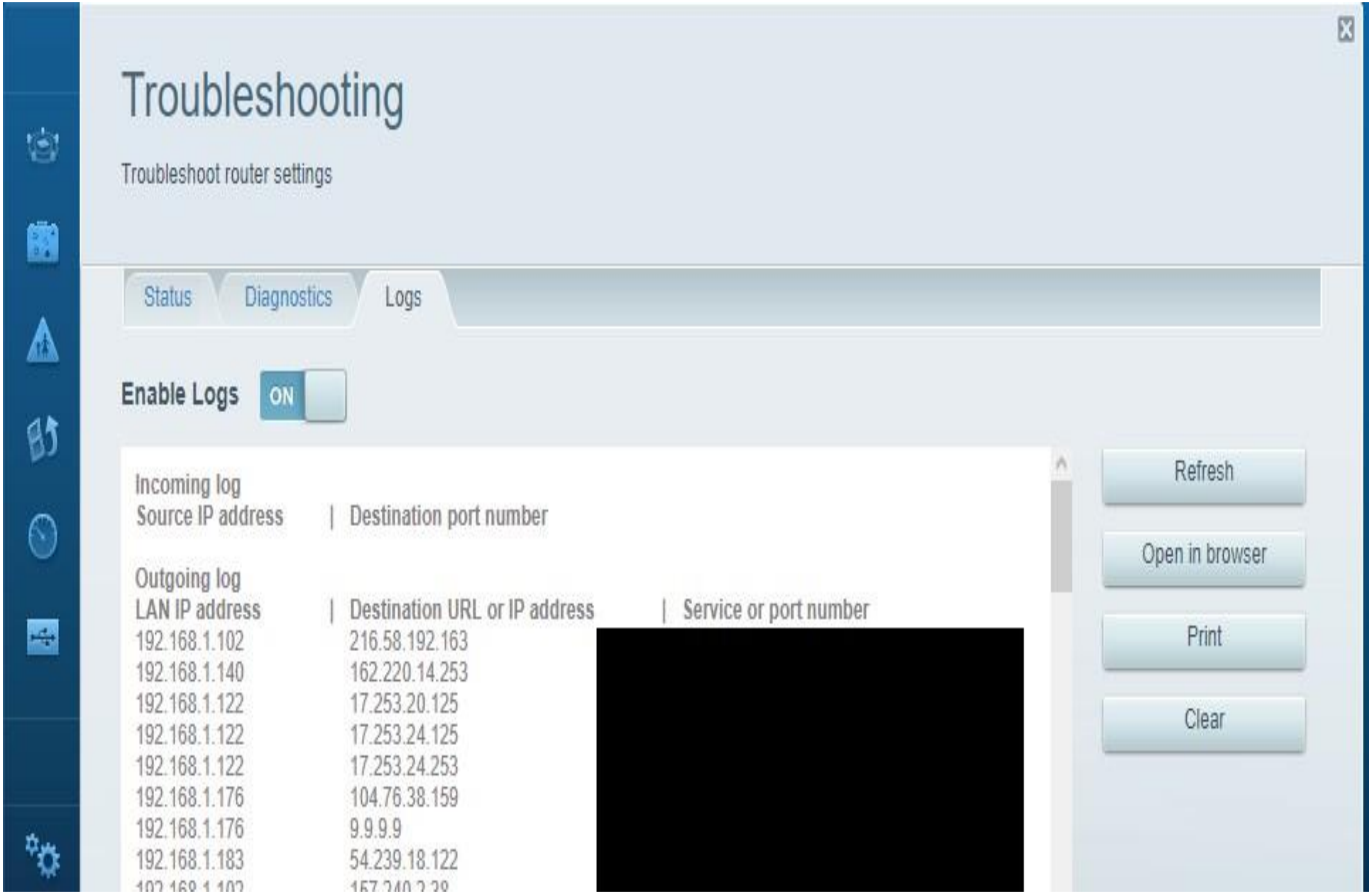
- Hardware Instrumentation – Network tap

  Privacy, a lot of data
- WEB proxy

  WEB traffic only
- Browser history

  WEB traffic only
- Internet router / Firewall logs

Logging to Identify issues



Troubleshooting

Troubleshoot router settings

Enable Logs ON

```
Incoming log
Source IP address      |  Destination port number

Outgoing log
LAN IP address         |  Destination URL or IP address      |  Service or port number
192.168.1.102             216.58.192.163
192.168.1.140             162.220.14.253
192.168.1.122             17.253.20.125
192.168.1.122             17.253.24.125
192.168.1.122             17.253.24.253
192.168.1.176             104.76.38.159
192.168.1.176             9.9.9.9
192.168.1.183             54.239.18.122
192.168.1.102             157.240.2.38
```

[redacted]

Logging to Identify issues

- Hardware Instrumentation – Network tap

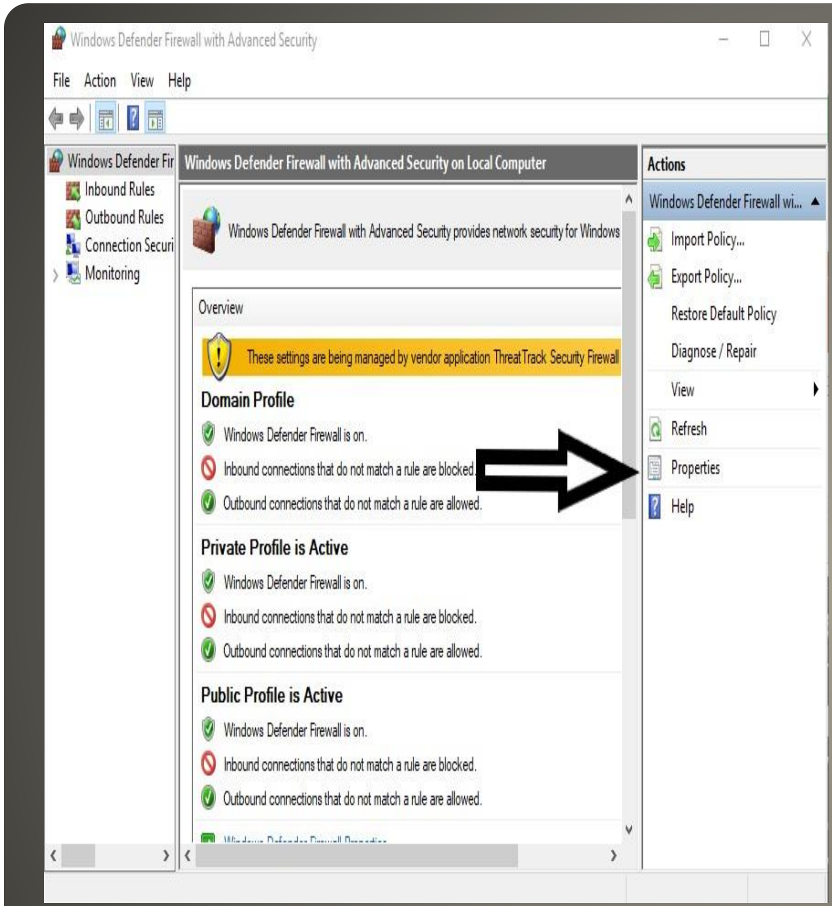
  Privacy, a lot of data
- WEB proxy

  WEB traffic only
- Browser history

  WEB traffic only
- Internet router / Firewall logs
- Operating system firewall log

  Disabled by default   can grow quite large

  wf.msc at run prompt



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows

Overview

These settings are being managed by vendor application ThreatTrack Security Firewall

Domain Profile

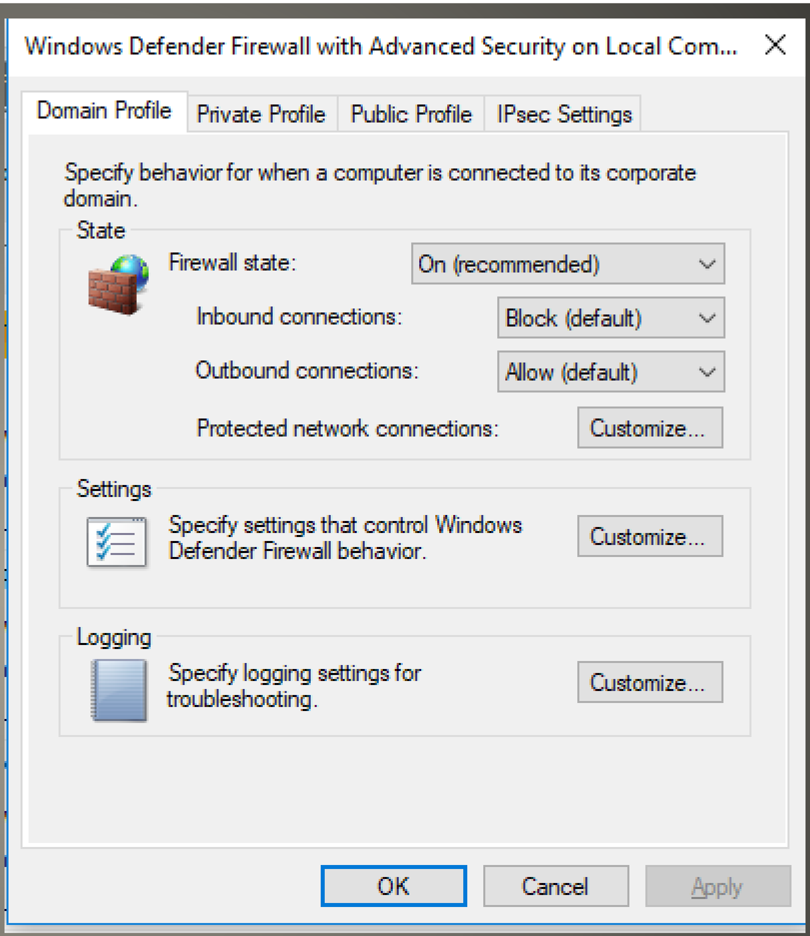
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.



Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

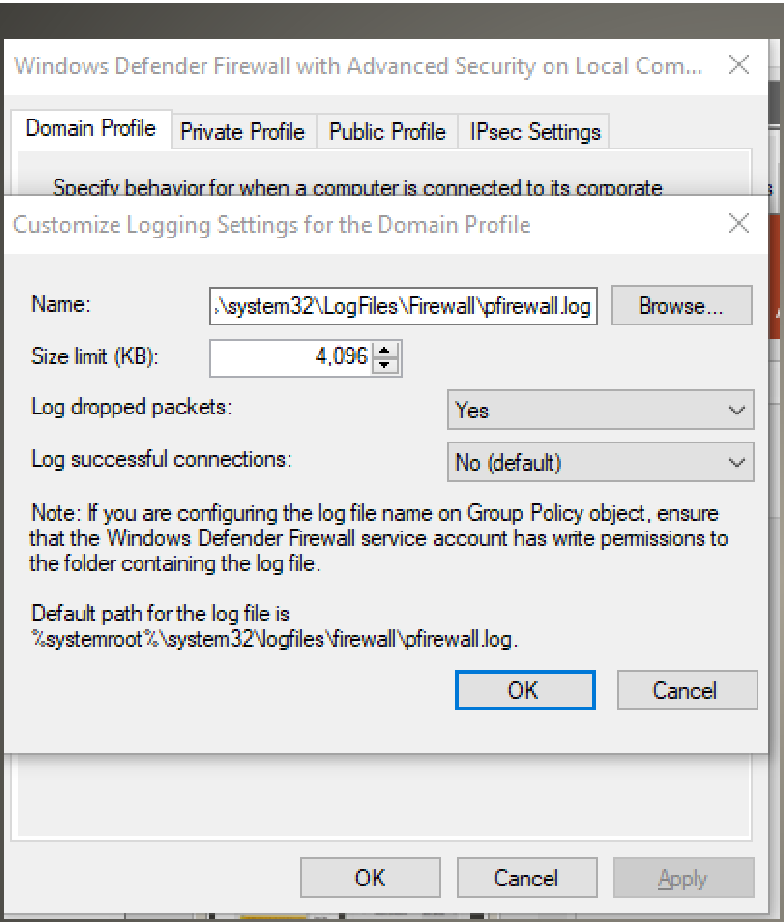
Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Windows firewall logging



Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate

Customize Logging Settings for the Domain Profile

Name: .\system32\LogFiles\Firewall\pfirewall.log

Size limit (KB): 4,096

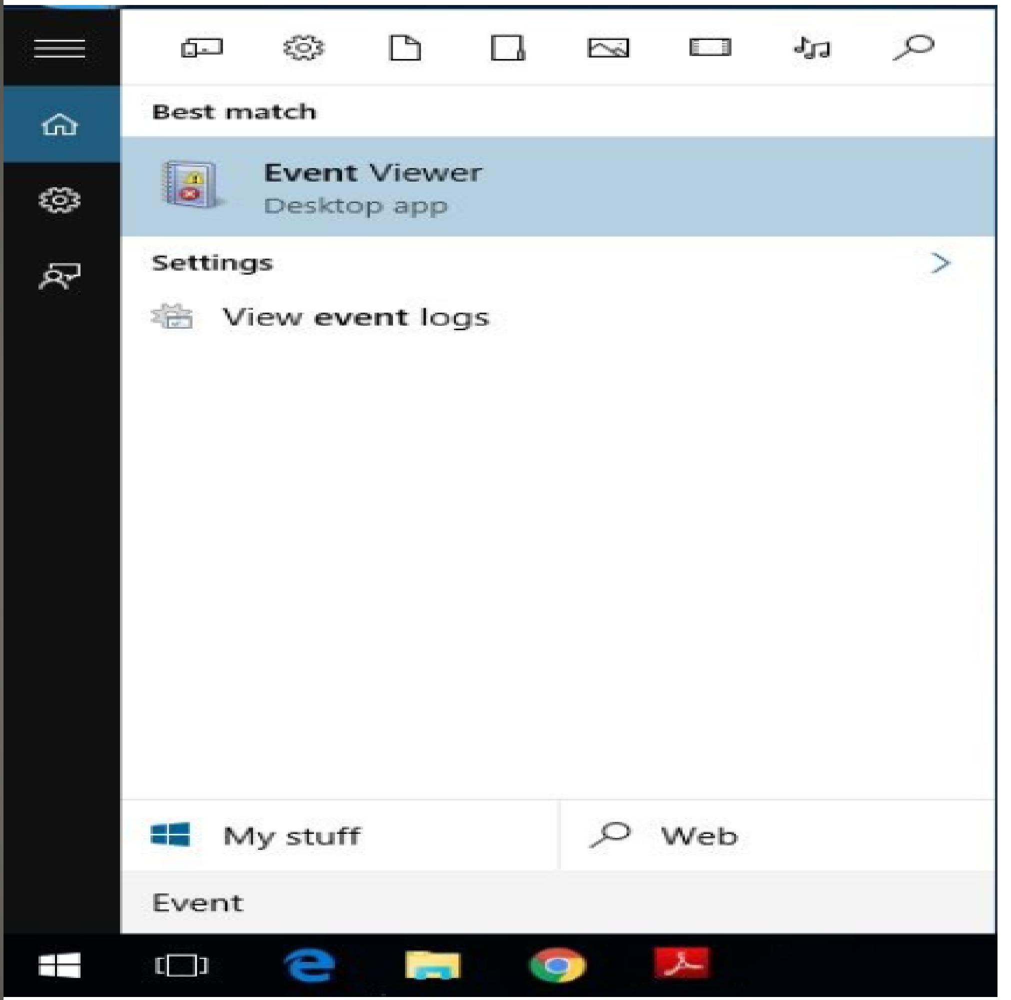
Log dropped packets: Yes

Log successful connections: No (default)

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

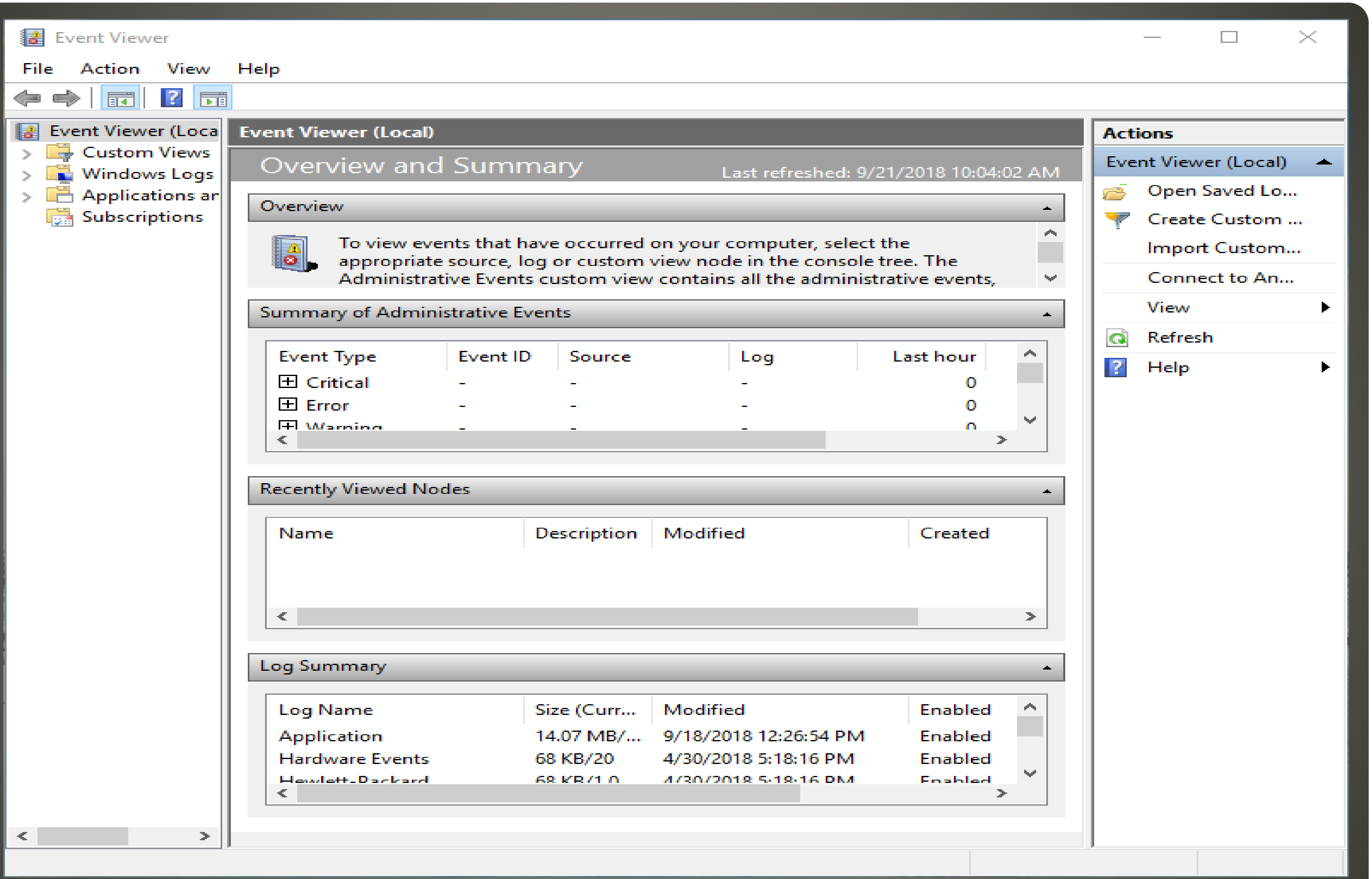
Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

Windows Firewall logging



Start Menu

Windows Event Viewer



Event Viewer (Local)

Overview and Summary

Last refreshed: 9/21/2018 10:04:02 AM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events,

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour
⊞ Critical	-	-	-	0
⊞ Error	-	-	-	0
⊞ Warning	-	-	-	0

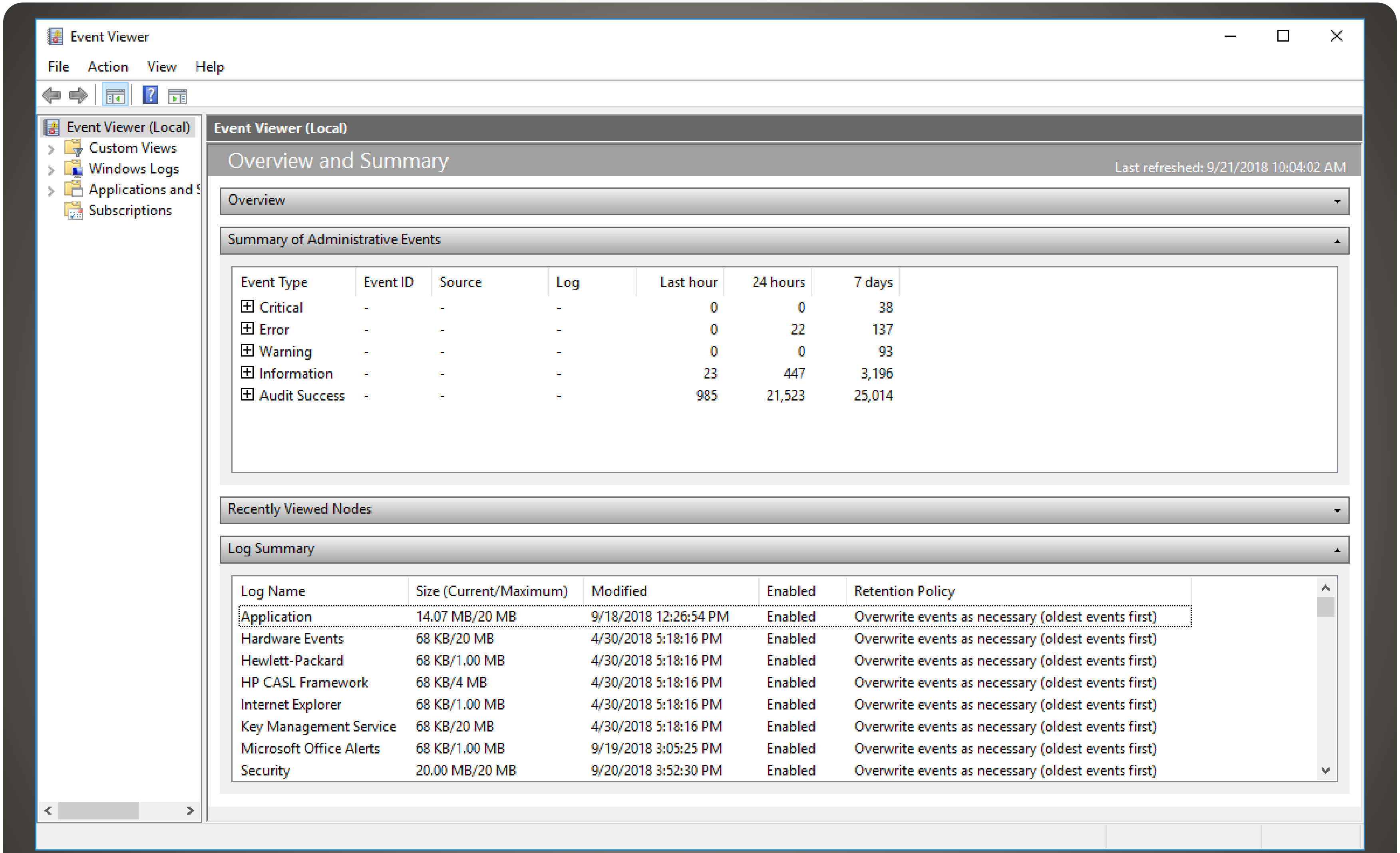
Recently Viewed Nodes

Name	Description	Modified	Created

Log Summary

Log Name	Size (Curr...	Modified	Enabled
Application	14.07 MB/...	9/18/2018 12:26:54 PM	Enabled
Hardware Events	68 KB/20	4/30/2018 5:18:16 PM	Enabled
Hewlett-Packard	68 KB/1.0	4/30/2018 5:18:16 PM	Enabled

Run as Administrator



Last refreshed: 9/21/2018 10:04:02 AM

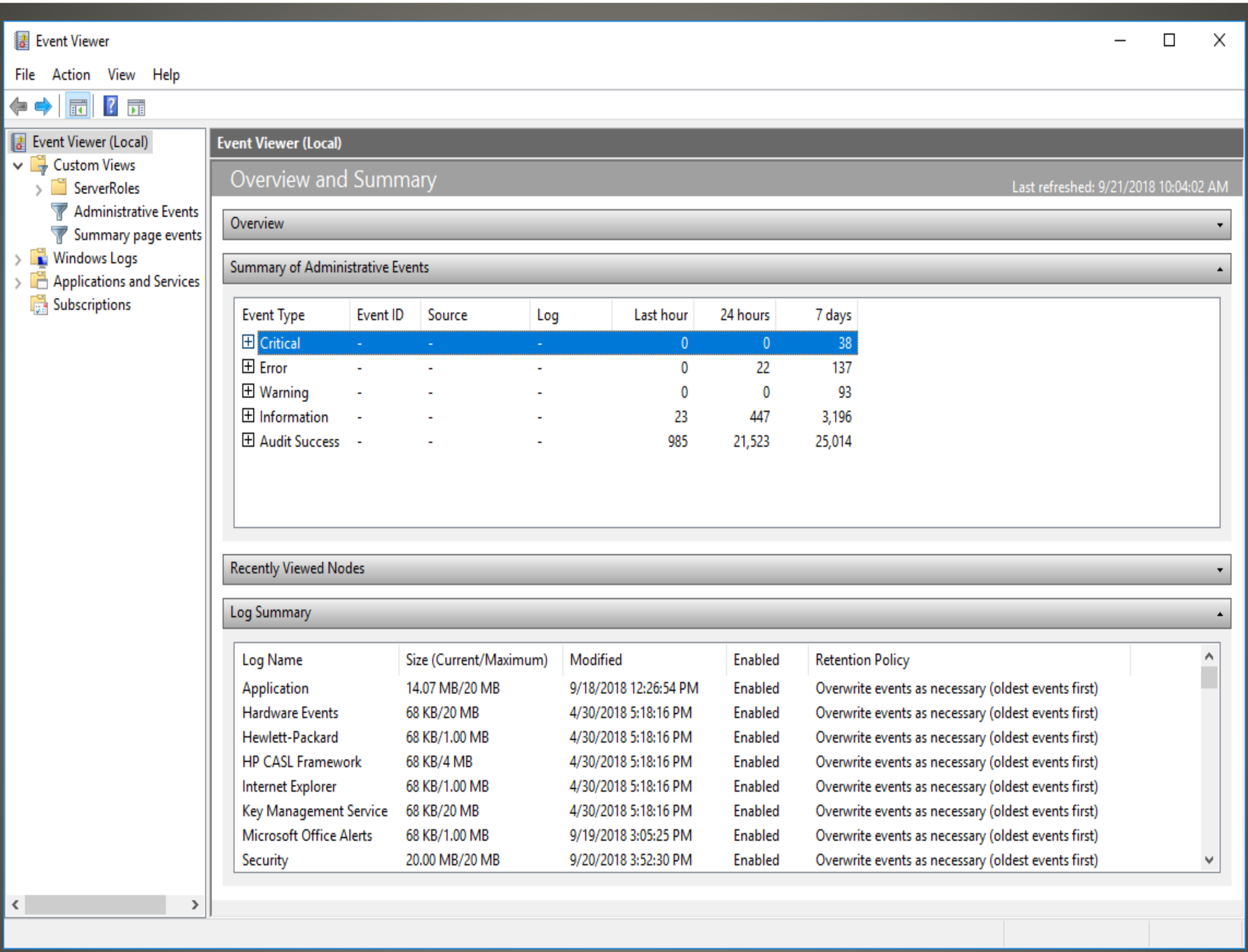
Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Critical	-	-	-	0	0	38
⊞ Error	-	-	-	0	22	137
⊞ Warning	-	-	-	0	0	93
⊞ Information	-	-	-	23	447	3,196
⊞ Audit Success	-	-	-	985	21,523	25,014

Log Summary

Log Name	Size (Current/Maximum)	Modified	Enabled	Retention Policy
Application	14.07 MB/20 MB	9/18/2018 12:26:54 PM	Enabled	Overwrite events as necessary (oldest events first)
Hardware Events	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Hewlett-Packard	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
HP CASL Framework	68 KB/4 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Internet Explorer	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Key Management Service	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Microsoft Office Alerts	68 KB/1.00 MB	9/19/2018 3:05:25 PM	Enabled	Overwrite events as necessary (oldest events first)
Security	20.00 MB/20 MB	9/20/2018 3:52:30 PM	Enabled	Overwrite events as necessary (oldest events first)

Adjust View to your liking



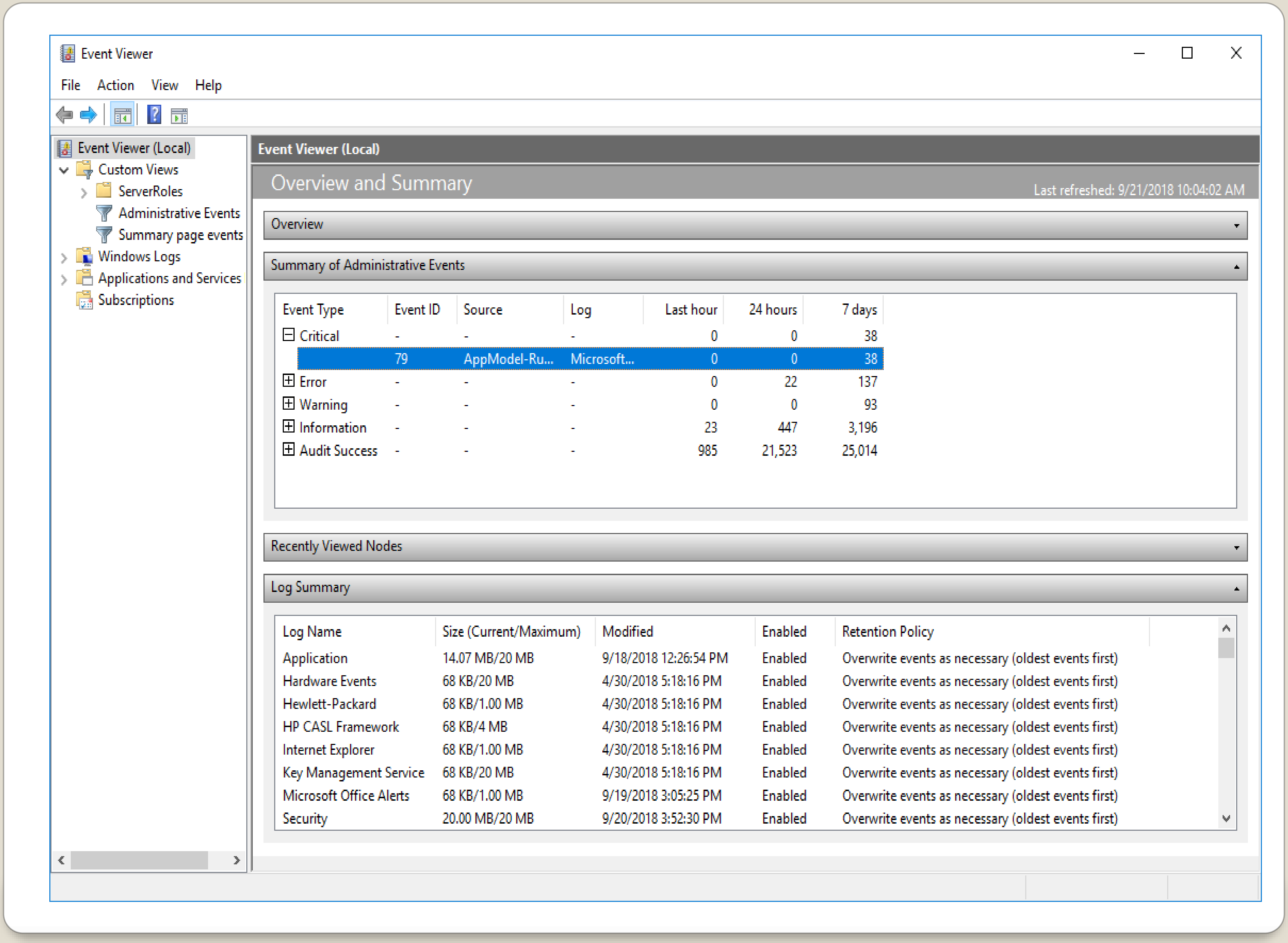
Overview and Summary

Last refreshed: 9/21/2018 10:04:02 AM

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Critical	-	-	-	0	0	38
⊞ Error	-	-	-	0	22	137
⊞ Warning	-	-	-	0	0	93
⊞ Information	-	-	-	23	447	3,196
⊞ Audit Success	-	-	-	985	21,523	25,014

Log Name	Size (Current/Maximum)	Modified	Enabled	Retention Policy
Application	14.07 MB/20 MB	9/18/2018 12:26:54 PM	Enabled	Overwrite events as necessary (oldest events first)
Hardware Events	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Hewlett-Packard	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
HP CASL Framework	68 KB/4 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Internet Explorer	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Key Management Service	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Microsoft Office Alerts	68 KB/1.00 MB	9/19/2018 3:05:25 PM	Enabled	Overwrite events as necessary (oldest events first)
Security	20.00 MB/20 MB	9/20/2018 3:52:30 PM	Enabled	Overwrite events as necessary (oldest events first)

Select by severity/importance



Overview and Summary

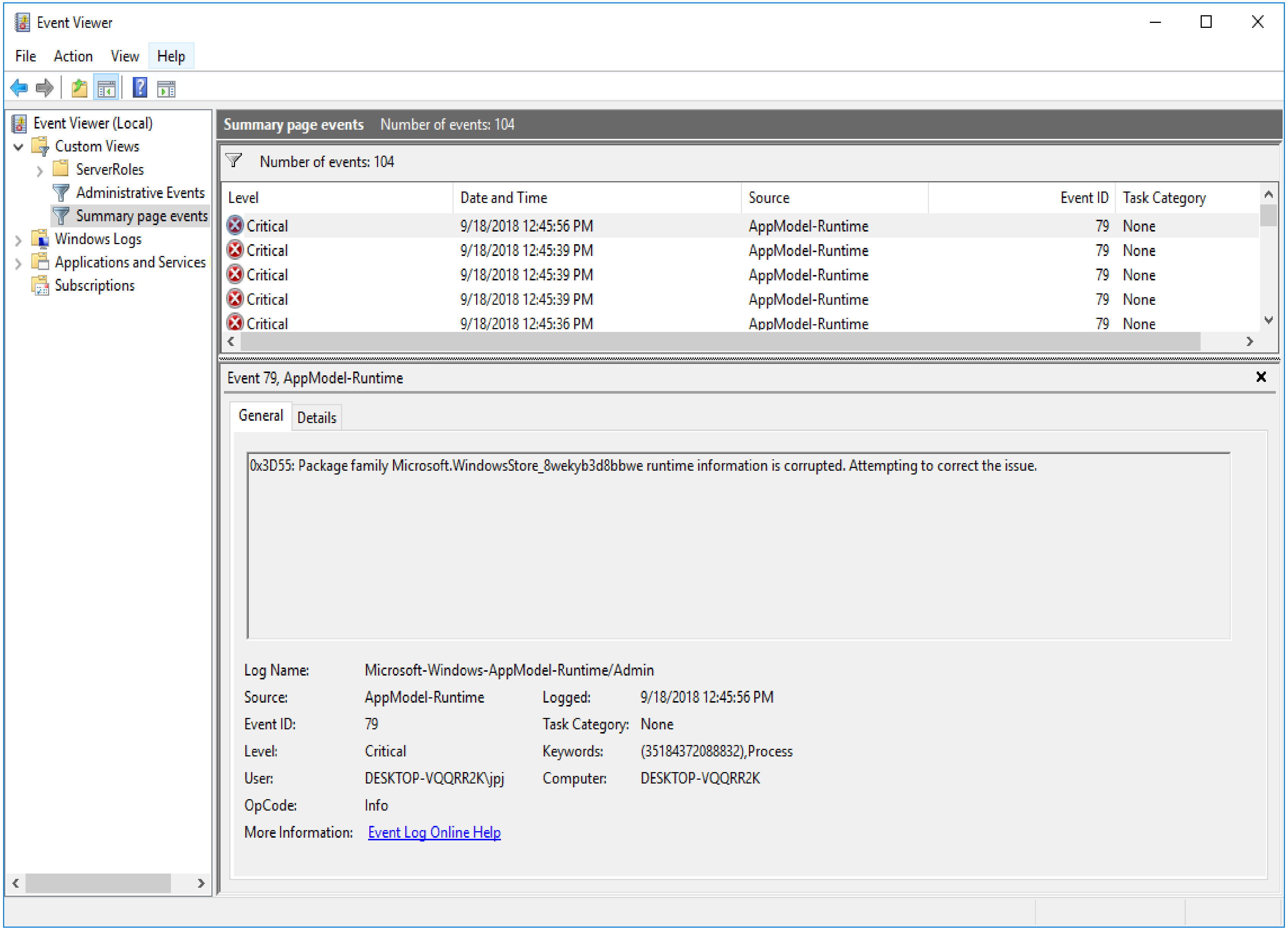
Last refreshed: 9/21/2018 10:04:02 AM

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊟ Critical	-	-	-	0	0	38
	79	AppModel-Ru...	Microsoft...	0	0	38
⊞ Error	-	-	-	0	22	137
⊞ Warning	-	-	-	0	0	93
⊞ Information	-	-	-	23	447	3,196
⊞ Audit Success	-	-	-	985	21,523	25,014

Log Summary

Log Name	Size (Current/Maximum)	Modified	Enabled	Retention Policy
Application	14.07 MB/20 MB	9/18/2018 12:26:54 PM	Enabled	Overwrite events as necessary (oldest events first)
Hardware Events	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Hewlett-Packard	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
HP CASL Framework	68 KB/4 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Internet Explorer	68 KB/1.00 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Key Management Service	68 KB/20 MB	4/30/2018 5:18:16 PM	Enabled	Overwrite events as necessary (oldest events first)
Microsoft Office Alerts	68 KB/1.00 MB	9/19/2018 3:05:25 PM	Enabled	Overwrite events as necessary (oldest events first)
Security	20.00 MB/20 MB	9/20/2018 3:52:30 PM	Enabled	Overwrite events as necessary (oldest events first)



Summary page events Number of events: 104

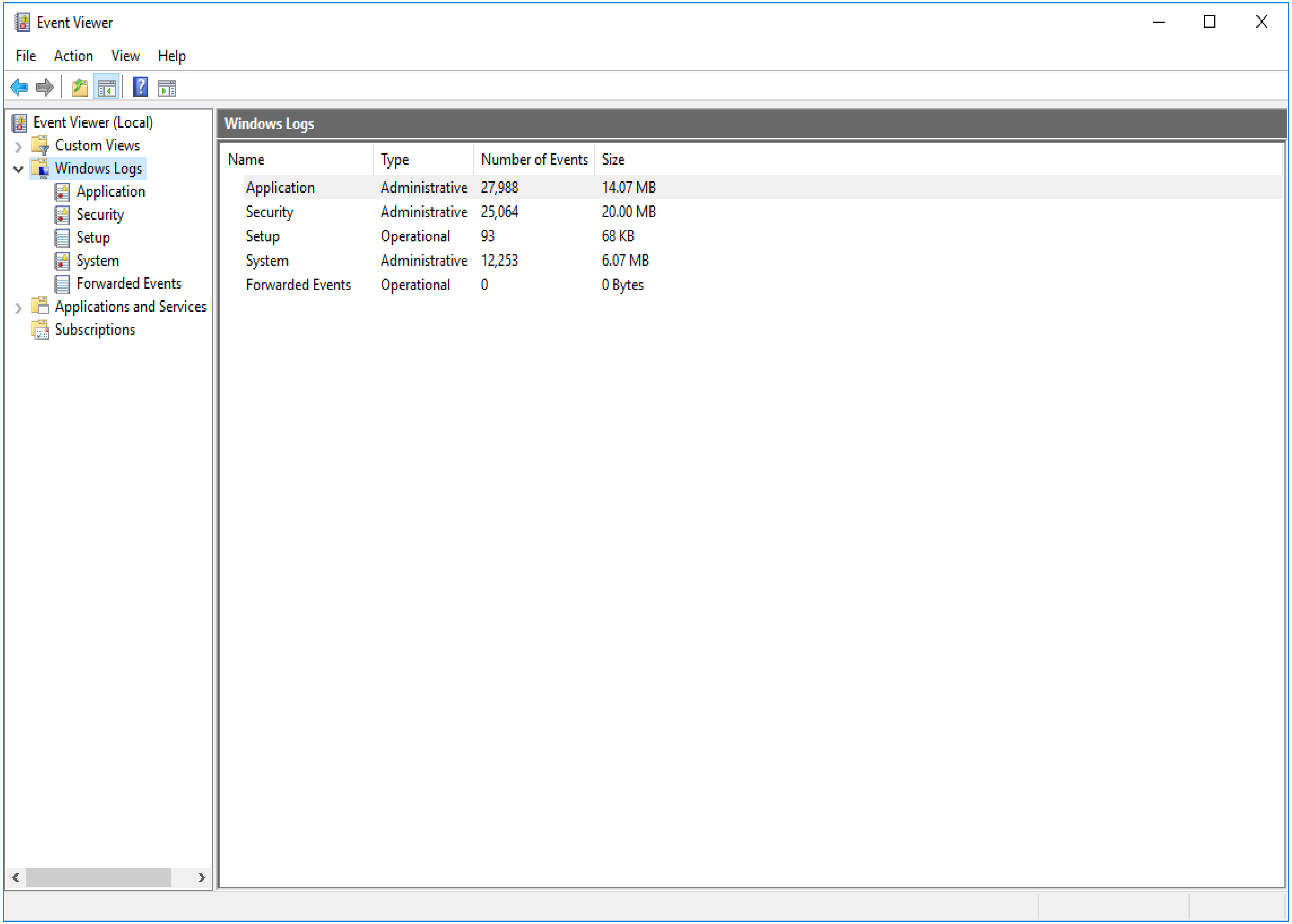
Number of events: 104

Level	Date and Time	Source	Event ID	Task Category
Critical	9/18/2018 12:45:56 PM	AppModel-Runtime	79	None
Critical	9/18/2018 12:45:39 PM	AppModel-Runtime	79	None
Critical	9/18/2018 12:45:39 PM	AppModel-Runtime	79	None
Critical	9/18/2018 12:45:39 PM	AppModel-Runtime	79	None
Critical	9/18/2018 12:45:36 PM	AppModel-Runtime	79	None

Event 79, AppModel-Runtime

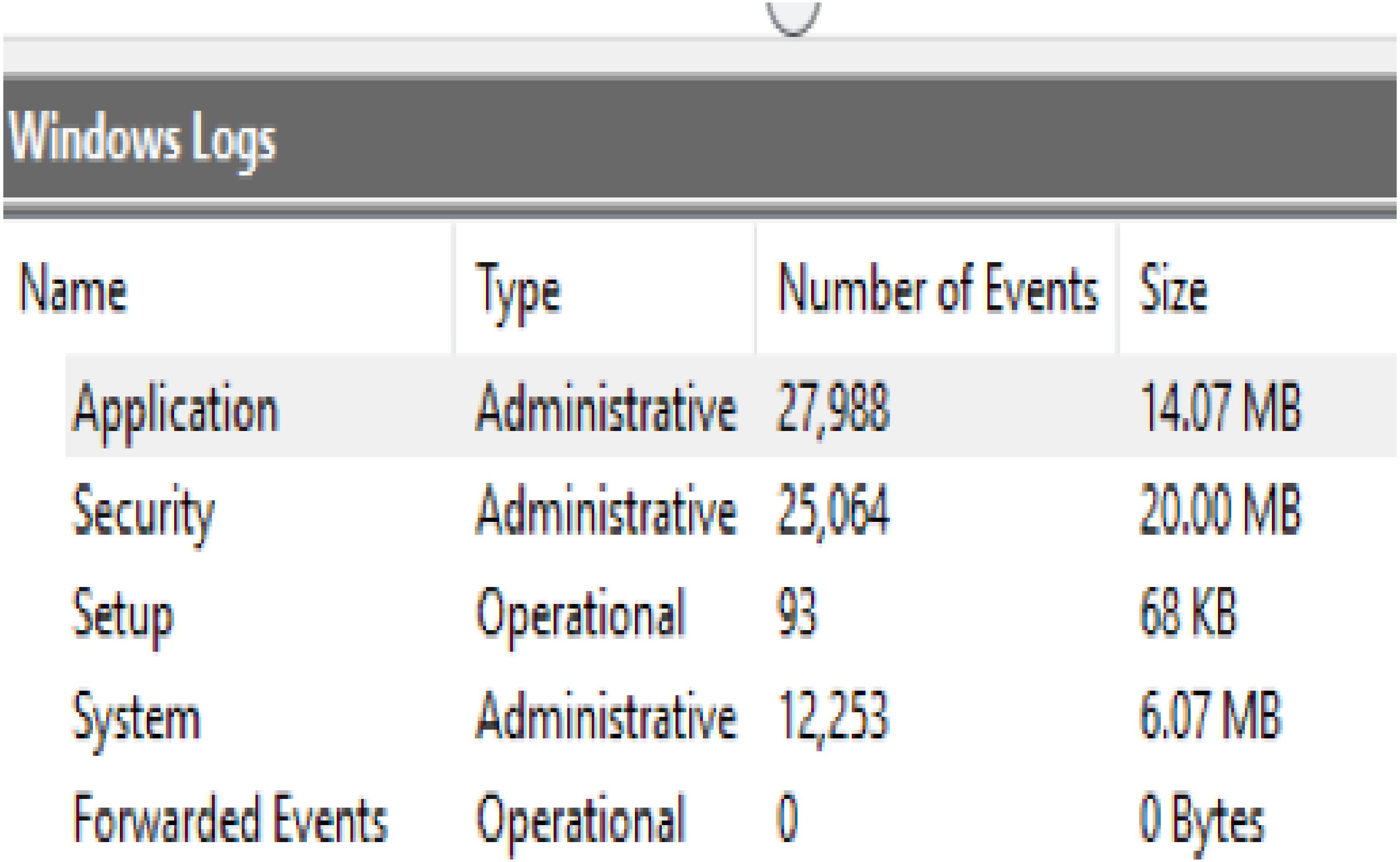
0x3D55: Package family Microsoft.WindowsStore_8wekyb3d8bbwe runtime information is corrupted. Attempting to correct the issue.

Log Name:	Microsoft-Windows-AppModel-Runtime/Admin		
Source:	AppModel-Runtime	Logged:	9/18/2018 12:45:56 PM
Event ID:	79	Task Category:	None
Level:	Critical	Keywords:	(35184372088832),Process
User:	DESKTOP-VQQRR2K\jpj	Computer:	DESKTOP-VQQRR2K
OpCode:	Info		
More Information:	Event Log Online Help		



Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	27,988	14.07 MB
Security	Administrative	25,064	20.00 MB
Setup	Operational	93	68 KB
System	Administrative	12,253	6.07 MB
Forwarded Events	Operational	0	0 Bytes

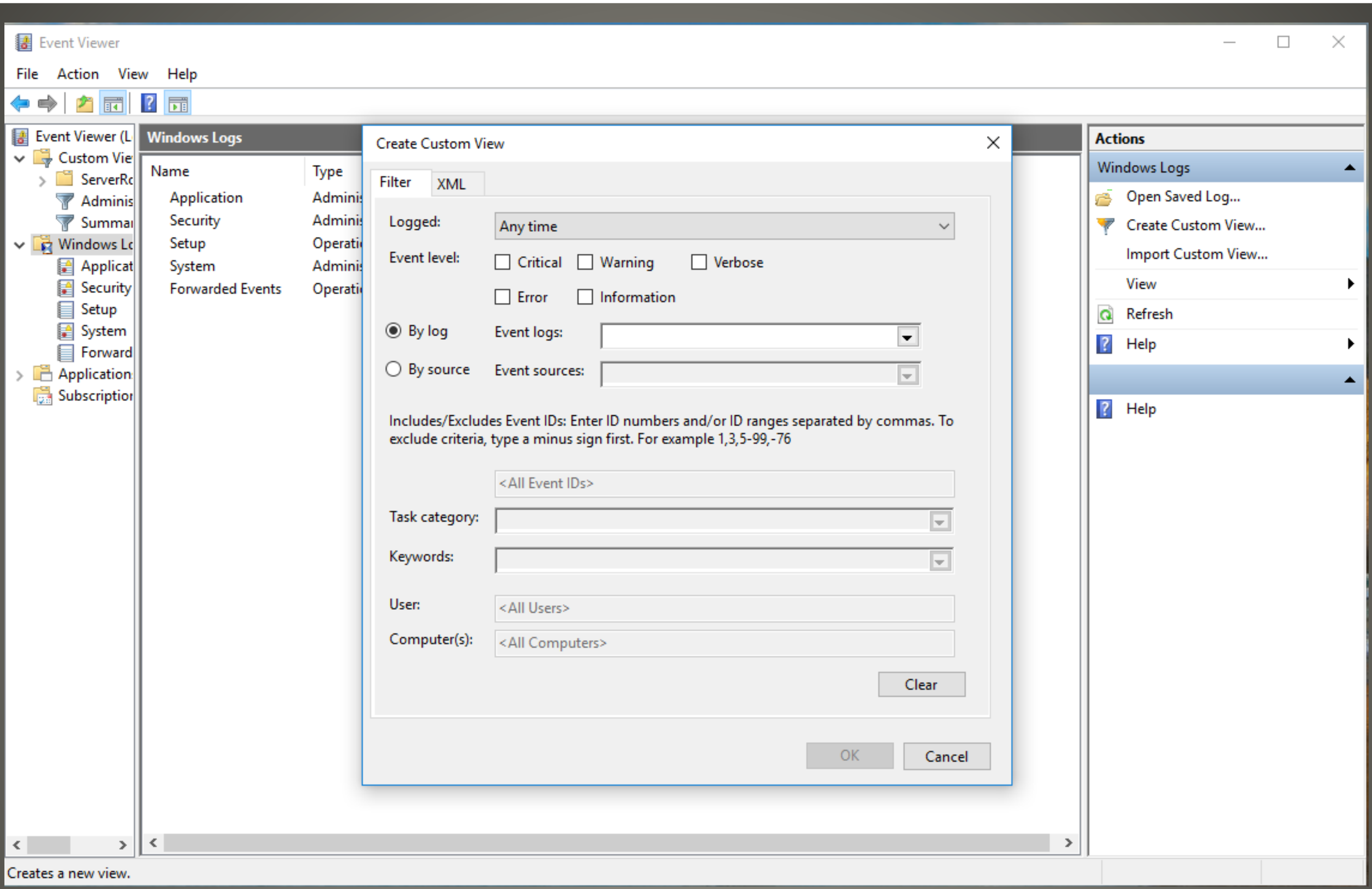


Windows Logs

Name	Type	Number of Events	Size
Application	Administrative	27,988	14.07 MB
Security	Administrative	25,064	20.00 MB
Setup	Operational	93	68 KB
System	Administrative	12,253	6.07 MB
Forwarded Events	Operational	0	0 Bytes

- Custom Views
- Clear and control logs and log sizes
- Save and Delete logs
- Create events with subscriptions

Windows Event Viewer



Create Custom View

Filter | XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs:

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

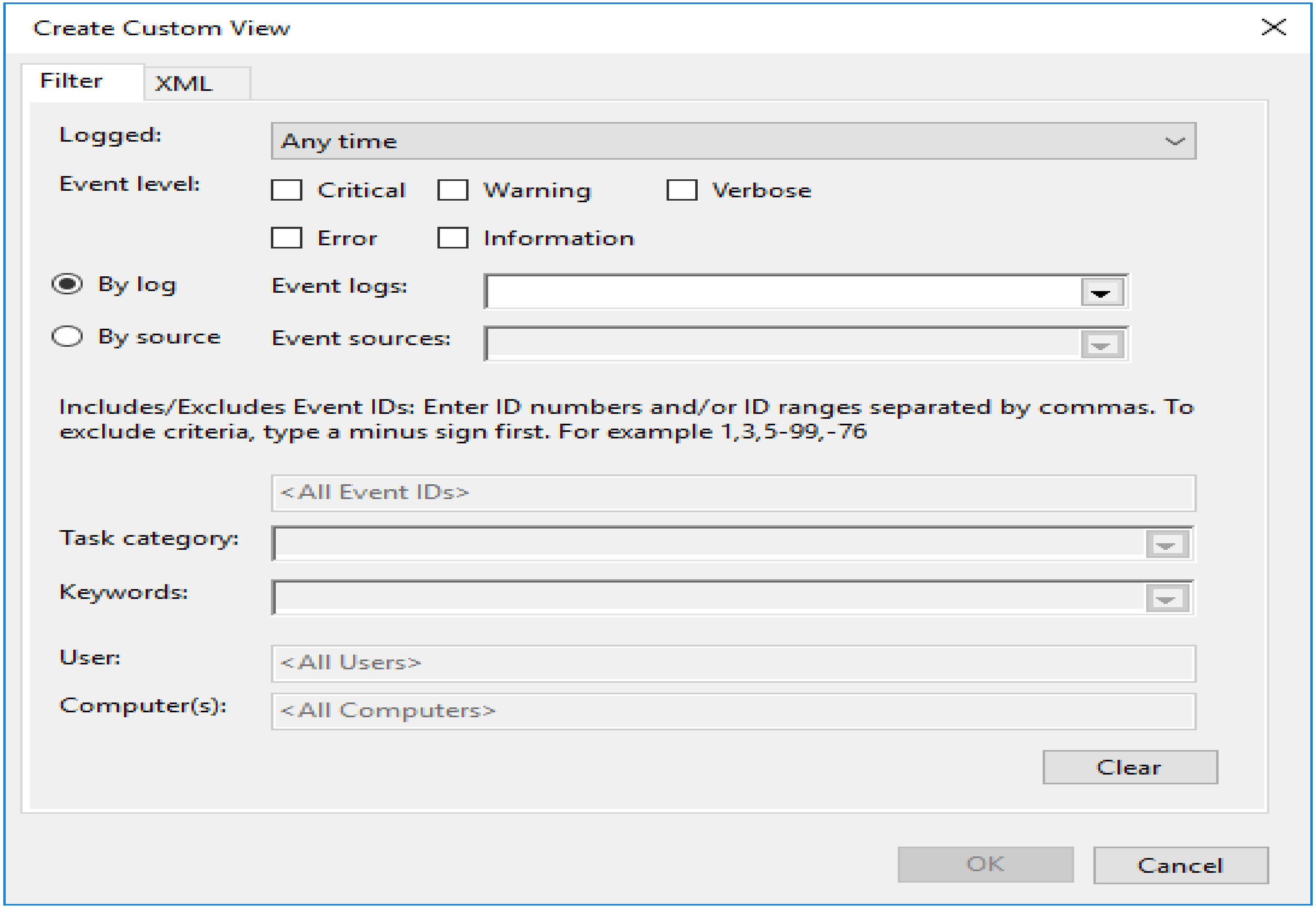
Keywords:

User: <All Users>

Computer(s): <All Computers>

Creates a new view.

Custom view



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs:

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

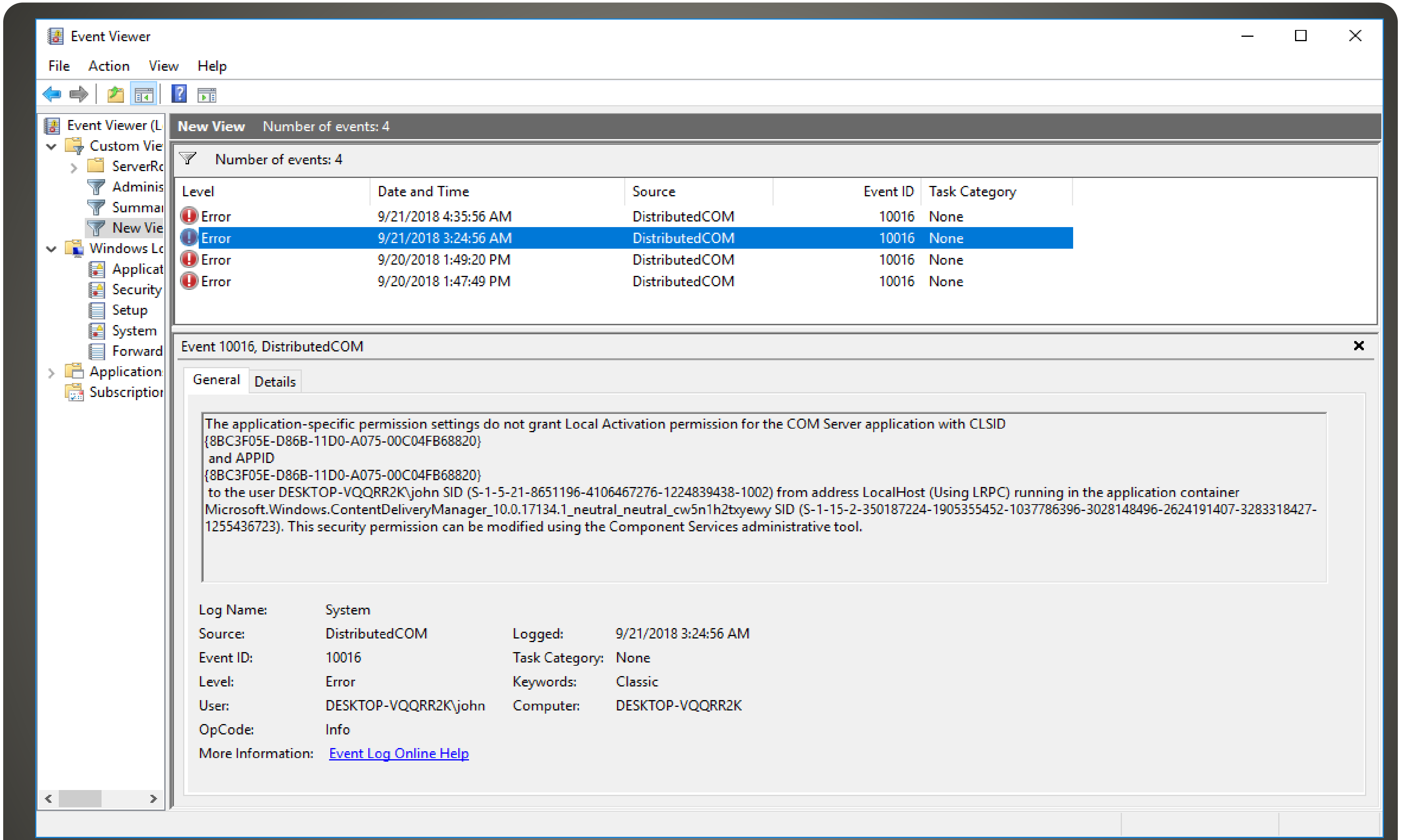
<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>



Number of events: 4

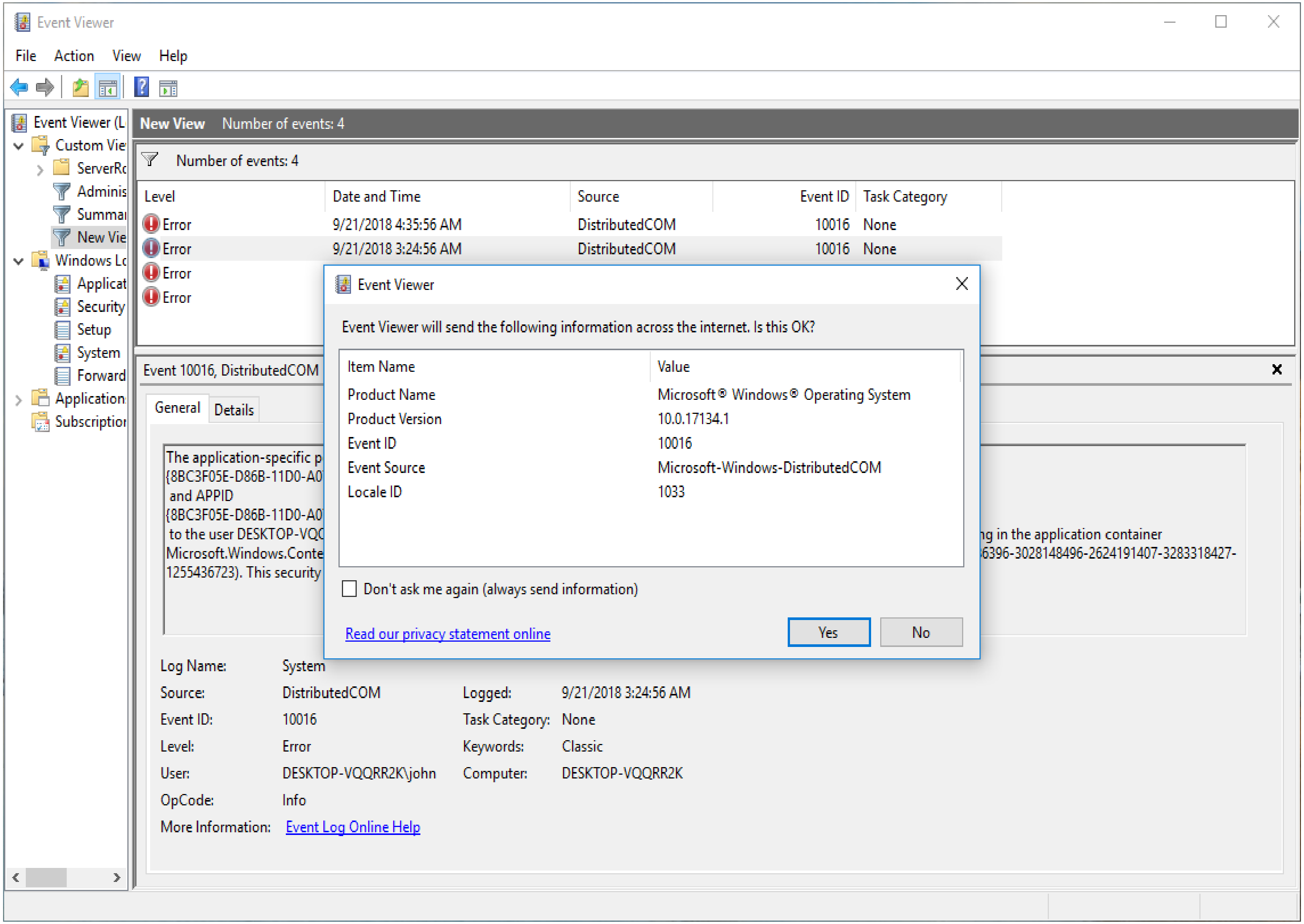
Level	Date and Time	Source	Event ID	Task Category
Error	9/21/2018 4:35:56 AM	DistributedCOM	10016	None
Error	9/21/2018 3:24:56 AM	DistributedCOM	10016	None
Error	9/20/2018 1:49:20 PM	DistributedCOM	10016	None
Error	9/20/2018 1:47:49 PM	DistributedCOM	10016	None

Event 10016, DistributedCOM

```
The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
{8BC3F05E-D86B-11D0-A075-00C04FB68820}
 and APPID
{8BC3F05E-D86B-11D0-A075-00C04FB68820}
 to the user DESKTOP-VQQRR2K\john SID (S-1-5-21-8651196-4106467276-1224839438-1002) from address LocalHost (Using LRPC) running in the application container
Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-350187224-1905355452-1037786396-3028148496-2624191407-3283318427-
1255436723). This security permission can be modified using the Component Services administrative tool.
```

Log Name:	System		
Source:	DistributedCOM	Logged:	9/21/2018 3:24:56 AM
Event ID:	10016	Task Category:	None
Level:	Error	Keywords:	Classic
User:	DESKTOP-VQQRR2K\john	Computer:	DESKTOP-VQQRR2K
OpCode:	Info		
More Information:	Event Log Online Help		

A custom view example



Number of events: 4

Level	Date and Time	Source	Event ID	Task Category
Error	9/21/2018 4:35:56 AM	DistributedCOM	10016	None
Error	9/21/2018 3:24:56 AM	DistributedCOM	10016	None
Error				
Error				

Event 10016, DistributedCOM

The application-specific p
{8BC3F05E-D86B-11D0-A0
and APPID
{8BC3F05E-D86B-11D0-A0
to the user DESKTOP-VQQ
Microsoft.Windows.Conte
1255436723). This security

ng in the application container
6396-3028148496-2624191407-3283318427-

Event Viewer

Event Viewer will send the following information across the internet. Is this OK?

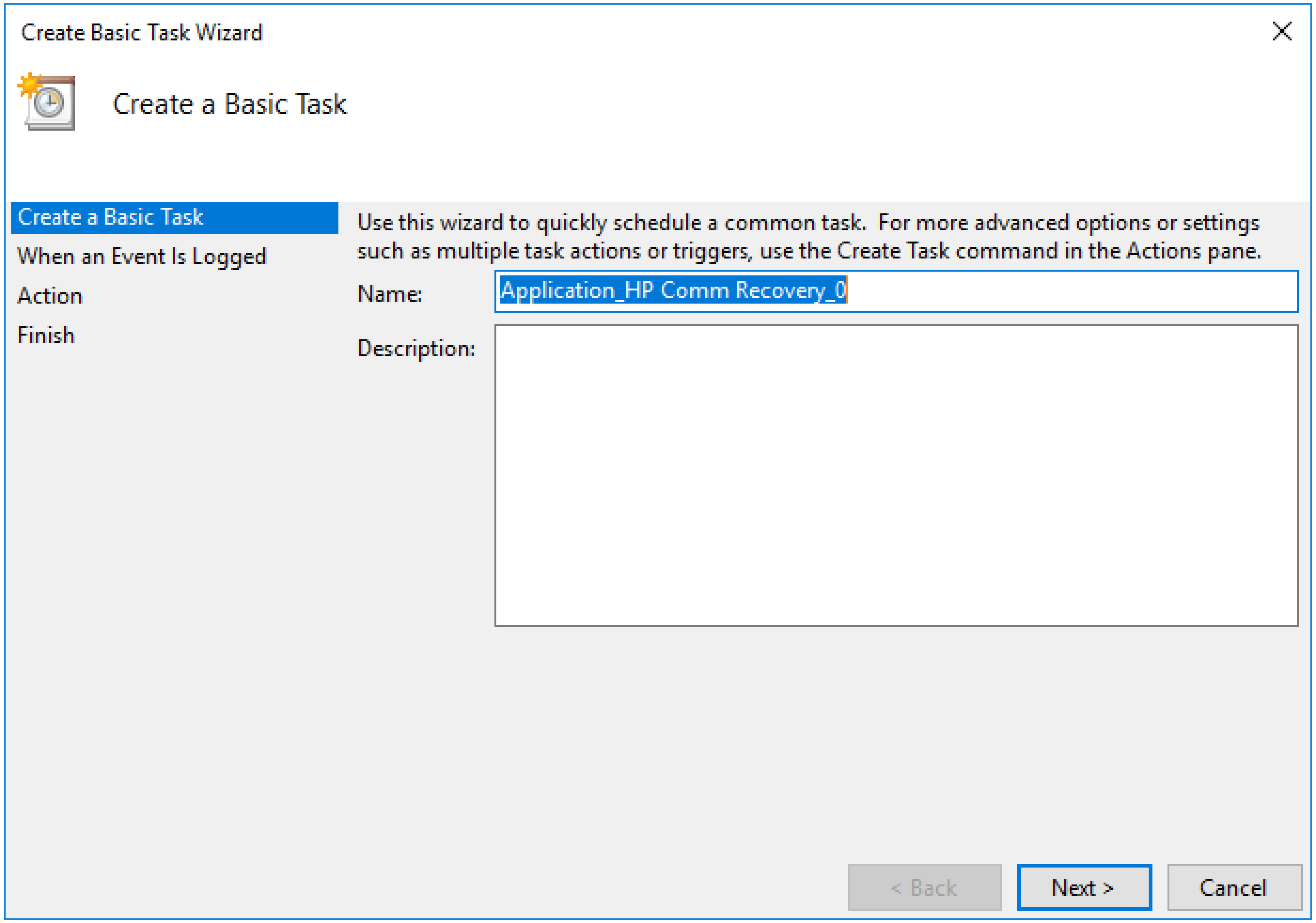
Item Name	Value
Product Name	Microsoft® Windows® Operating System
Product Version	10.0.17134.1
Event ID	10016
Event Source	Microsoft-Windows-DistributedCOM
Locale ID	1033

□ Don't ask me again (always send information)

Read our privacy statement online

Yes No

Log Name:	System		
Source:	DistributedCOM	Logged:	9/21/2018 3:24:56 AM
Event ID:	10016	Task Category:	None
Level:	Error	Keywords:	Classic
User:	DESKTOP-VQQRR2K\john	Computer:	DESKTOP-VQQRR2K
OpCode:	Info		
More Information:	Event Log Online Help		

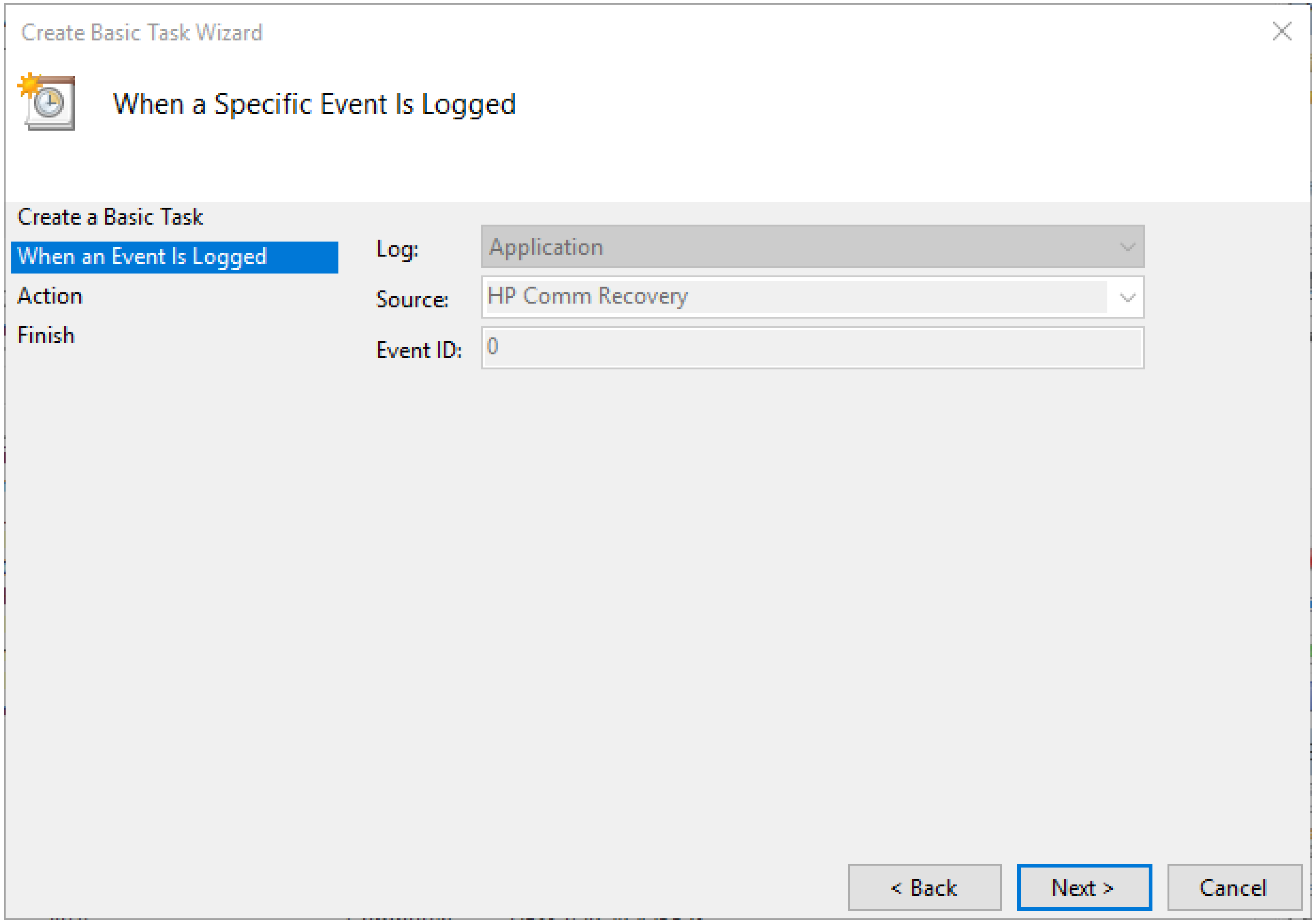


Create a Basic Task

Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: Application_HP Comm Recovery_0

Description:



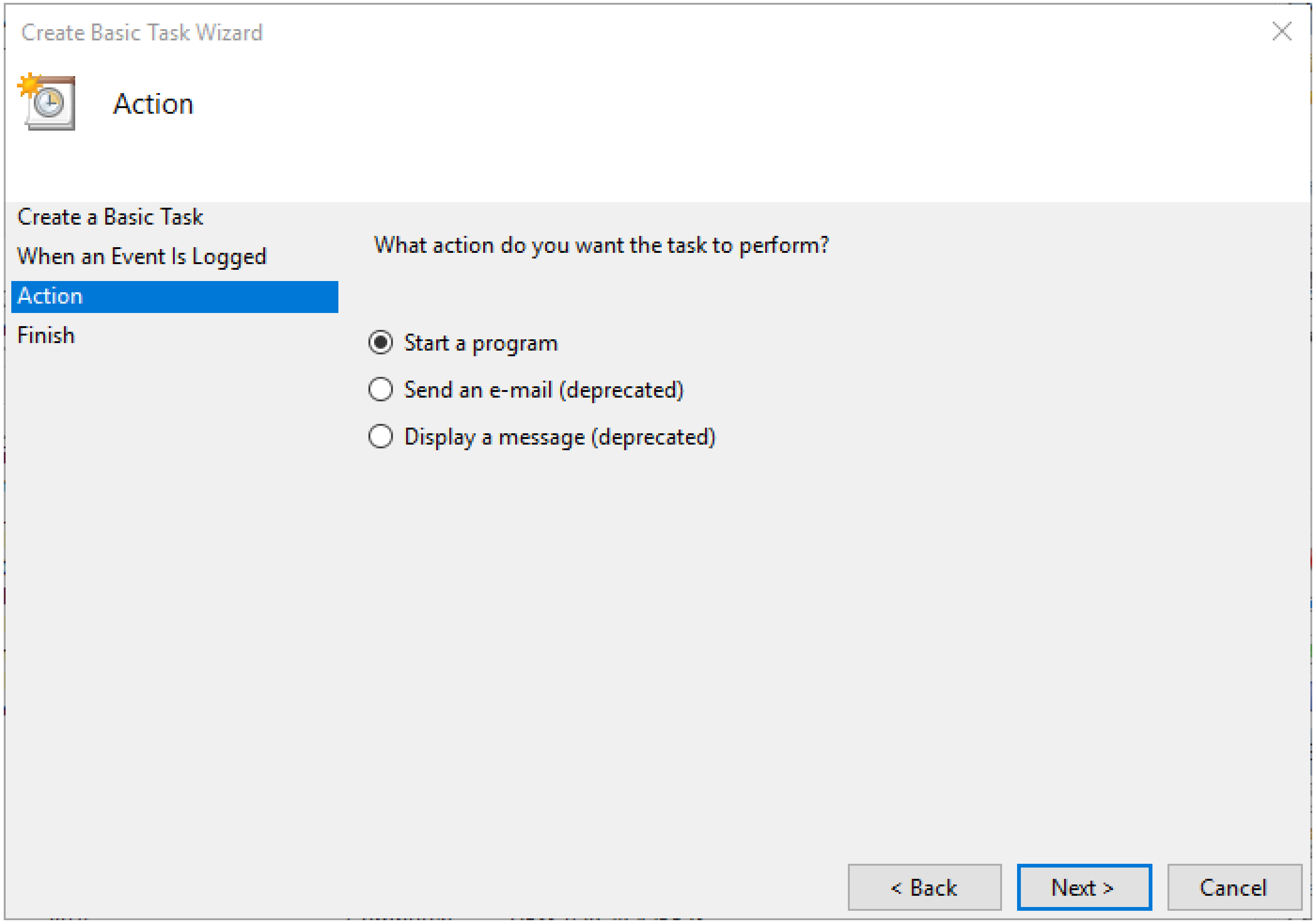
Create Basic Task Wizard

When a Specific Event Is Logged

Log: Application

Source: HP Comm Recovery

Event ID: 0

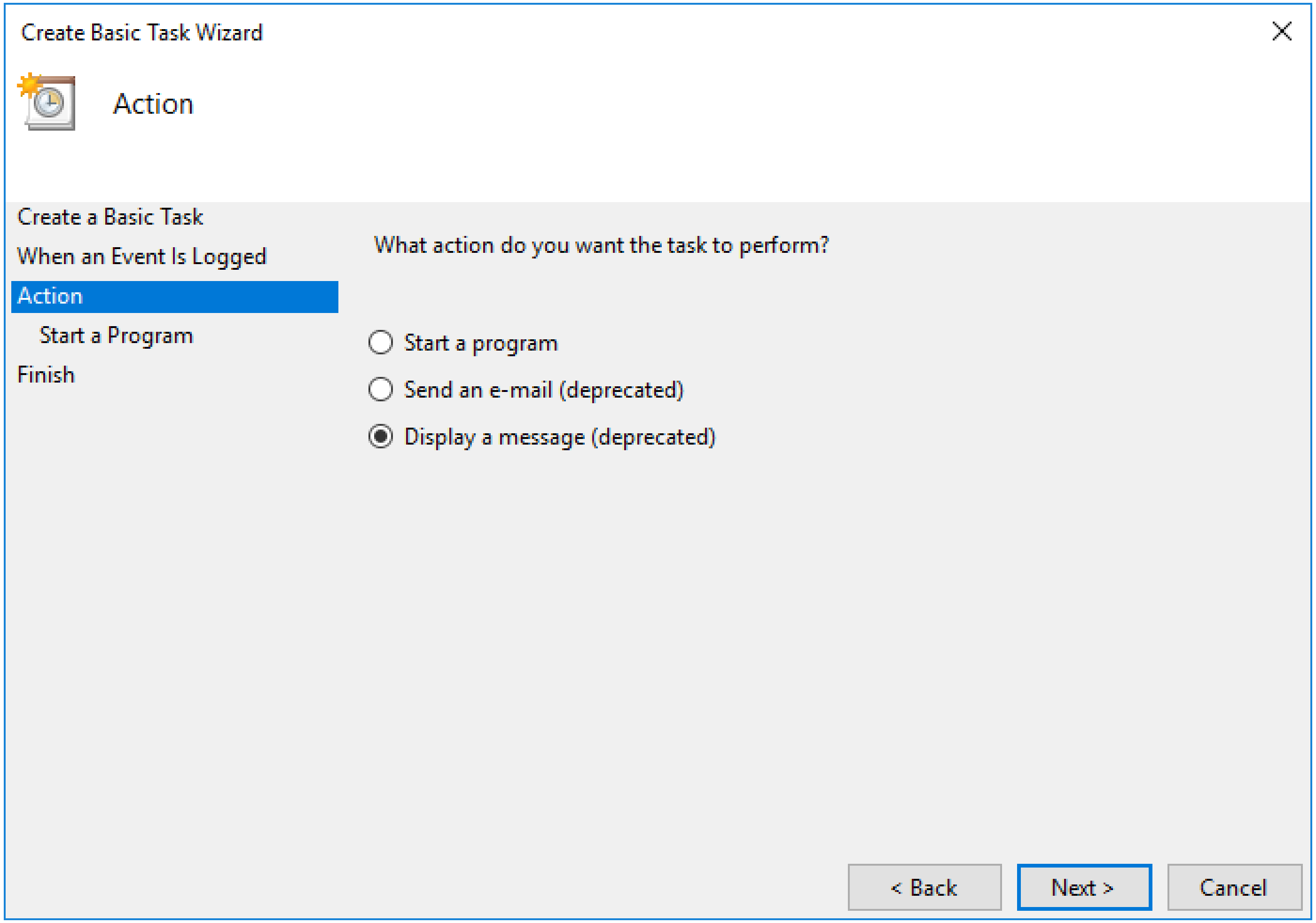


What action do you want the task to perform?

● Start a program

○ Send an e-mail (deprecated)

○ Display a message (deprecated)



Create Basic Task Wizard

Action

What action do you want the task to perform?

○ Start a program

○ Send an e-mail (deprecated)

● Display a message (deprecated)

- Questions, suggestions, comments?
- Please wait for microphone
- Next Meeting October 23
- Help with Chairs You know the drill
  front row to front of room
  stack 7 high

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer Safe enough?
- Do nothing no problem
  <most of us>
- Do everything - catastrophic