

# MEMUG Scotland

18<sup>th</sup> October 2022



@MemugScotland



<https://memug.scot>



**Beyond Native Reporting!**

## Speaker Info

# Maurice Daly



Principal Cloud Architect at **CloudWay**, and a Microsoft MVP in the area of Enterprise Mobility since 2017.

Twitter - **@modaly\_it**

Blog – **MSEndpointMgr Blog** – <https://www.msendpointmgr.com>

(Yes we do know about the name change 🤔 )

Interests – Formula 1, all things IT..

# YOUR EXPERIENCE – INTUNE REPORTS

## Intune Reporting

Historically this has been the unloved area of Microsoft ~~Endpo~~.. I mean Intune. It has improved recently, but typically this is what I hear

- **The Good**
  - Endpoint Analytics reporting
- **The Bad**
  - Number inconsistencies
- **The Ugly**
  - Exportable formats

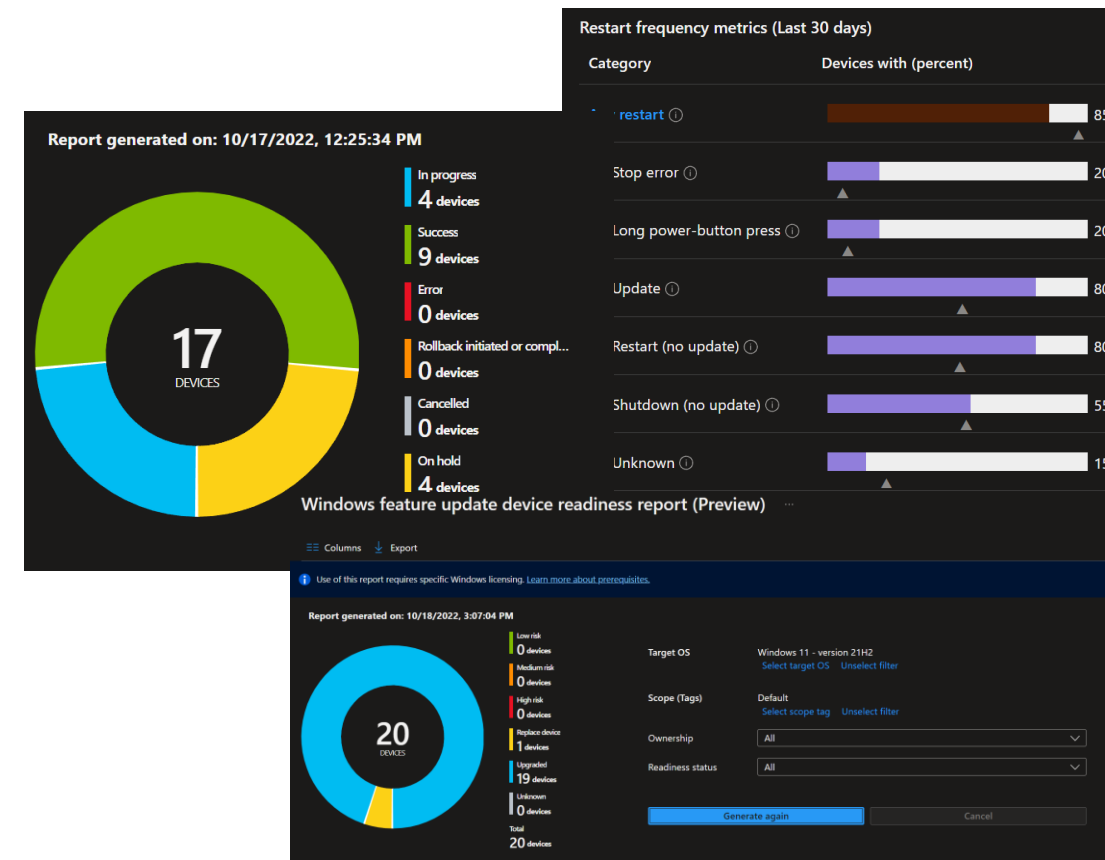


# INTUNE REPORTS – GETTING BETTER

## BUT ITS GETTING BETTER

Recent additions help admins get a clearer view of the world

- **Windows 10 and later feature updates**
  - Safeguard Hold Status
- **Feature Update Readiness**
  - Identify app, driver or hardware incompatibility
- **Endpoint Analytics**
  - Device and application performance, system reboots



# WHAT IS KUSTO QUERY LANGUAGE??

- **Kusto may refer to:**
  - Kustö, the Swedish name of Kuusisto (island), Finland
  - Marek Kusto (born 1954), Polish football player
  - **Microsoft Kusto, a query language used in Azure Data Explorer**
- **KQL History**
  - Development started in 2014 as a Microsoft project to provide fast and scalable log and telemetry insights. With the internal code name 'Kusto' (named after Jacques Cousteau, as a reference to "exploring the ocean of data").
  - Microsoft announced a public preview of Azure Data Explorer at Ignite in 2018
  - <https://en.wikipedia.org/wiki/Kusto>

# YOU MIGHT REMEMBER KQL FROM SUCH THINGS AS...

- **CMPIvot**

- CMPIvot uses a subset of KQL, with some minor differences, but uses the same logic
- Useful queries include
  - **Find local administrators;**  
Administrators  
| where Name !Contains 'Administrator' and Name !contains 'Domain Admins'
  - **Installed Products;**  
InstalledSoftware | summarize dcount( Device ) by ProductName
  - **Clients not part of a boundary group;**  
CcmLog('LocationServices') | where LogText contains 'Client is not in any boundary group.' | project Device, LogText, DateTime

- **Sentinel**



# WHY SHOULD I USE KQL FOR REPORTING?

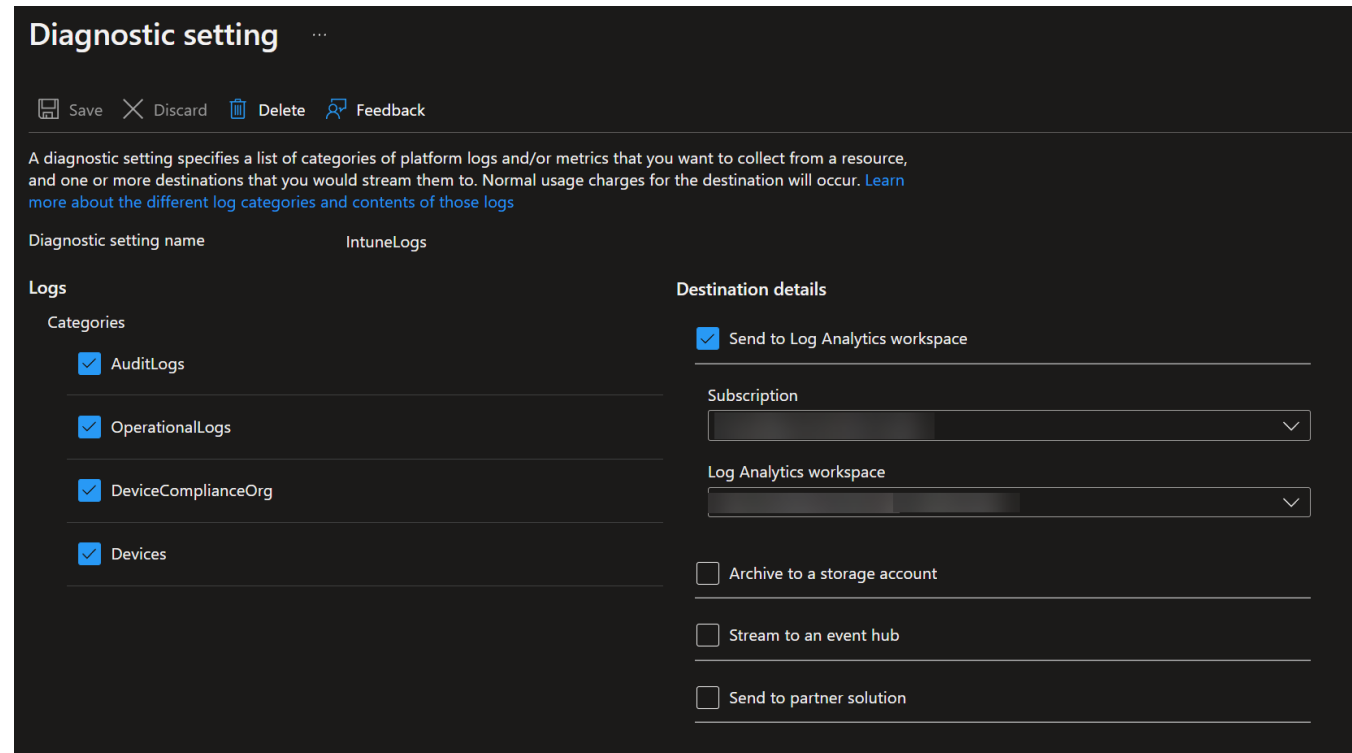
- **Compliance Reporting**
  - Organisations require proof of mitigation against security exploits
- **Native Export Formats**
  - Detected applications, awesome CSV files FTW?
- **PowerBI You Say**
  - My head hurt and now I need a license
- **Management**
  - You're rebuilding a failed exchange server? That's nice, could you please give me a report and have it for a meeting I have in 30 minutes?



# FIRST THINGS FIRST – (This “might” cost money)

**BEFORE** we go custom creating KQL queries and workbooks, we **NEED** a Log Analytics workspace

- **Requirement(s)**
  - Azure Subscription
  - Resource Group / Owner, or GA rights to provision the Log Analytics Workspace
  - Intune Admin / Global Admin rights to enable diagnostic settings both in Intune and Azure AD



The screenshot shows the 'Diagnostic setting' configuration page in the Azure portal. The setting name is 'IntuneLogs'. Under the 'Logs' section, four categories are selected: AuditLogs, OperationalLogs, DeviceComplianceOrg, and Devices. Under the 'Destination details' section, the 'Send to Log Analytics workspace' option is checked. The 'Subscription' and 'Log Analytics workspace' dropdowns are visible but not expanded. Other destination options like 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution' are unchecked.

**Diagnostic setting** ...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name: IntuneLogs

**Logs**

Categories

- ☒ AuditLogs
- ☒ OperationalLogs
- ☒ DeviceComplianceOrg
- ☒ Devices

**Destination details**

- ☒ Send to Log Analytics workspace
- Subscription: [Dropdown]
- Log Analytics workspace: [Dropdown]
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution



# THE BASICS – WHAT YOU NEED TO KNOW

- **Start querying your data:**

- *Search*
- *Where*
- *Limit/Take*
- *Count*
- *Project*
- *Distinct*
- *Render*
- *Order/Sort/Top*
- *Summarize*



# KQL EXAMPLES

- **Start querying your data:**

- *Search*
- *Where*
- *Limit/Take*
- *Count*
- *Project*
- *Distinct*
- *Render*
- *Order/Sort/Top*
- *Summarize*

## Some Examples

```
IntuneDevices  
| search "iOS"
```

```
IntuneAuditLogs  
| search "%User%"
```

```
AppInventory_CL  
| summarize dcount(ManagedDeviceID_g) by AppName_s,  
AppVersion_s, AppPublisher_s  
| order by dcount_ManagedDeviceID_g desc  
| take 5  
| render piechart
```

# MEMUG Scotland



**PATCH**  
MY PC

**DEMO TIME**



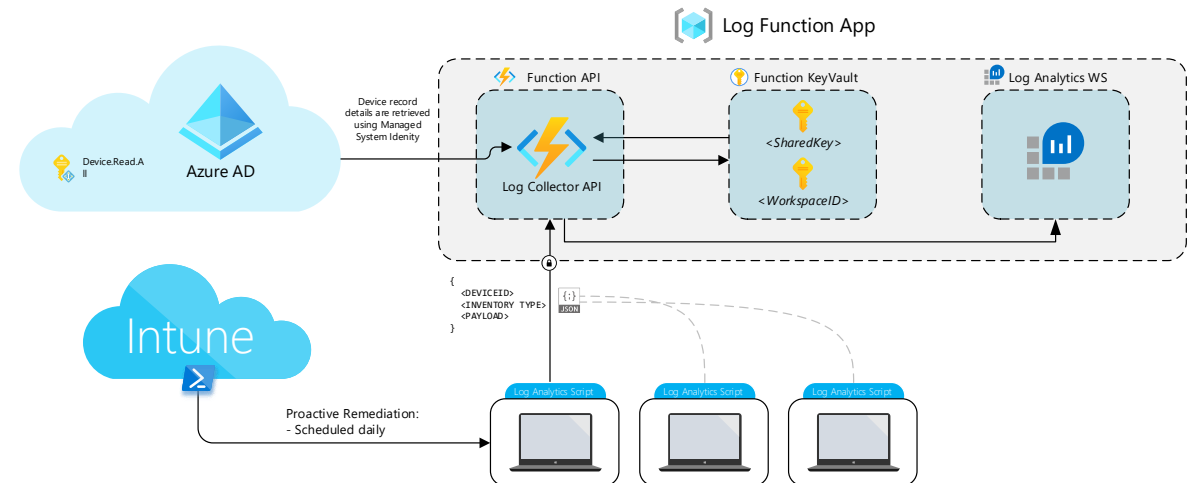
# Going CUSTOM – Function App

## What about custom data collection?

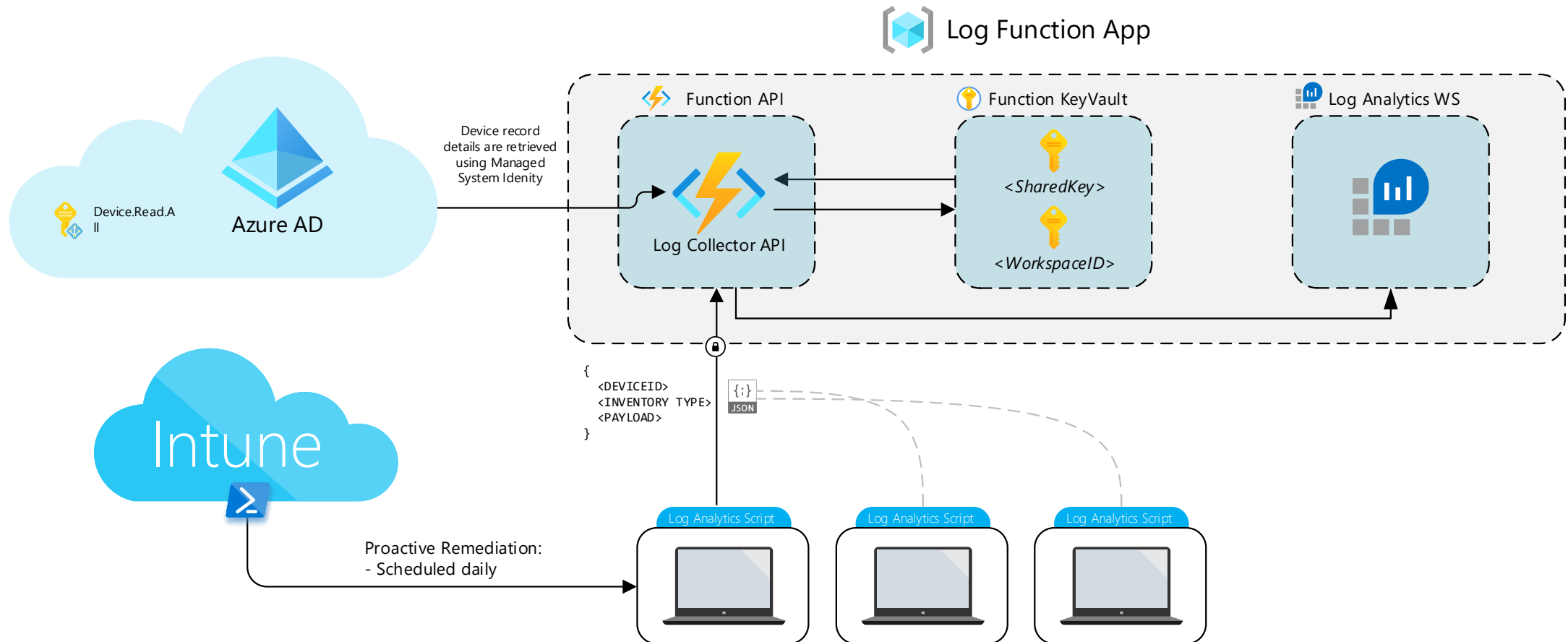
Jan Ketil Skanke has written a custom Azure function that allows you to gather application and device inventory information... But that is just the beginning

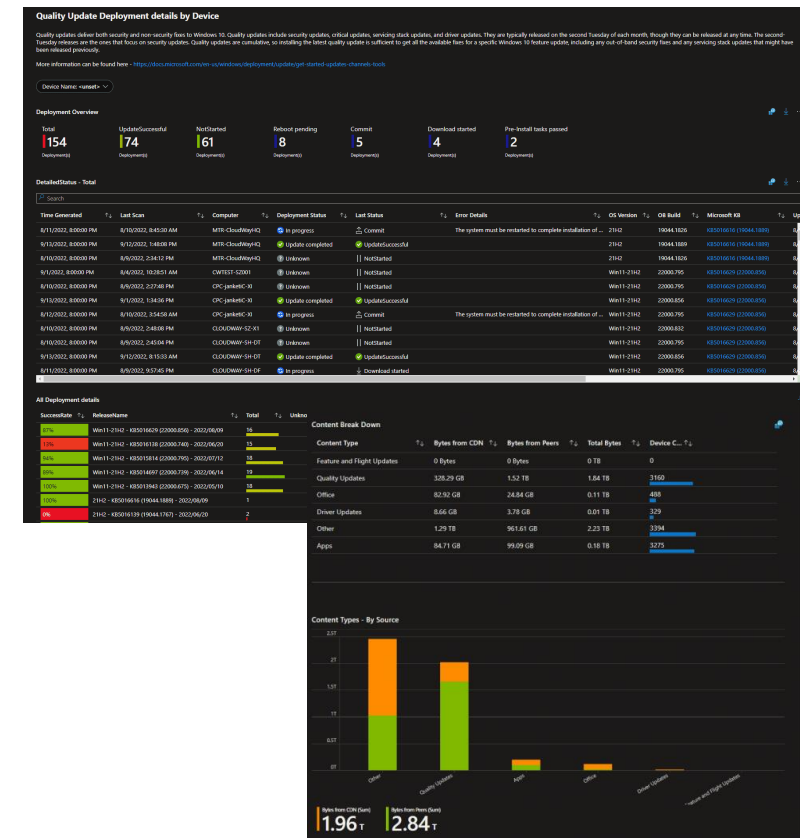
### Real World Applications

- Application Reliability
- AppLocker
- Driver Information
- BIOS Information
- Application Audit Events



# Going CUSTOM – Function App





# KQL Workbooks FTW!!!

## Quality Update Deployment details by Device

Quality updates deliver both security and non-security fixes to Windows 10. Quality updates include security updates, critical updates, servicing stack updates, and driver updates. They are typically released on the second Tuesday of each month, though they can be released at any time. The second-Tuesday releases are the ones that focus on security updates. Quality updates are cumulative, so installing the latest quality update is sufficient to get all the available fixes for a specific Windows 10 feature update, including any out-of-band security fixes and any servicing stack updates that might have been released previously.

More information can be found here - <https://docs.microsoft.com/en-us/windows/deployment/update/get-started-updates-channels-tools>

Device Name: <unset> ▾

### Deployment Overview

Total	UpdateSuccessful	NotStarted	Reboot pending	Commit	Download started	Pre-Install tasks passed
154	74	61	8	5	4	2
Deployment(s)	Deployment(s)	Deployment(s)	Deployment(s)	Deployment(s)	Deployment(s)	Deployment(s)

### DetailedStatus - Total

Search

Time Generated	Last Scan	Computer	Deployment Status	Last Status	Error Details	OS Version	OB Build	Microsoft K
8/11/2022, 8:00:00 PM	8/10/2022, 8:45:30 AM	MTR-CloudWayHQ	In progress	Commit	The system must be restarted to complete installation of ...	21H2	19044.1826	KB5016616
9/13/2022, 8:00:00 PM	9/12/2022, 1:48:08 PM	MTR-CloudWayHQ	Update completed	UpdateSuccessful		21H2	19044.1889	KB5016616
8/10/2022, 8:00:00 PM	8/9/2022, 2:34:12 PM	MTR-CloudWayHQ	Unknown	NotStarted		21H2	19044.1826	KB5016616
9/1/2022, 8:00:00 PM	8/4/2022, 10:28:51 AM	CWTEST-S2001	Unknown	NotStarted		Win11-21H2	22000.795	KB5016629
8/10/2022, 8:00:00 PM	8/9/2022, 2:27:48 PM	CPC-janketC-XI	Unknown	NotStarted		Win11-21H2	22000.795	KB5016629
9/13/2022, 8:00:00 PM	9/1/2022, 1:34:36 PM	CPC-janketC-XI	Update completed	UpdateSuccessful		Win11-21H2	22000.856	KB5016629
8/12/2022, 8:00:00 PM	8/10/2022, 3:54:58 AM	CPC-janketC-XI	In progress	Commit	The system must be restarted to complete installation of ...	Win11-21H2	22000.795	KB5016629
8/10/2022, 8:00:00 PM	8/9/2022, 2:48:08 PM	CLOUDWAY-SZ-X1	Unknown	NotStarted		Win11-21H2	22000.832	KB5016629
8/10/2022, 8:00:00 PM	8/9/2022, 2:45:04 PM	CLOUDWAY-SH-DT	Unknown	NotStarted		Win11-21H2	22000.795	KB5016629
9/13/2022, 8:00:00 PM	9/12/2022, 8:15:33 AM	CLOUDWAY-SH-DT	Update completed	UpdateSuccessful		Win11-21H2	22000.856	KB5016629
8/11/2022, 8:00:00 PM	8/9/2022, 9:57:45 PM	CLOUDWAY-SH-DF	In progress	Download started		Win11-21H2	22000.795	KB5016629

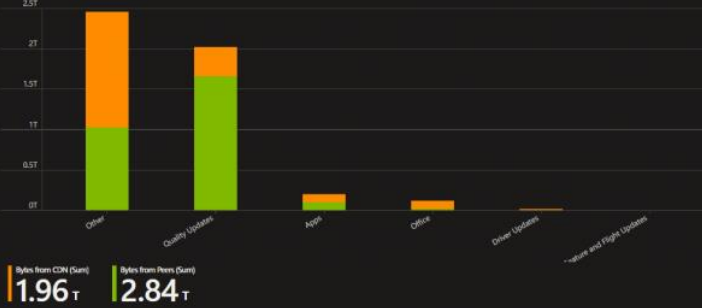
### All Deployment details

SuccessRate	ReleaseName	Total	Unkno...	Update completed
87%	Win11-21H2 - KB5016629 (22000.856) - 2022/08/09	16	2	14
13%	Win11-21H2 - KB5016138 (22000.740) - 2022/06/20	15	13	2
94%	Win11-21H2 - KB5015814 (22000.795) - 2022/07/12	18	1	17
89%	Win11-21H2 - KB5014697 (22000.739) - 2022/06/14	19	2	17
100%	Win11-21H2 - KB5013943 (22000.675) - 2022/05/10	18	0	18
100%	21H2 - KB5016616 (19044.1889) - 2022/08/09	1	0	1
0%	21H2 - KB5016139 (19044.1767) - 2022/06/20	2	2	0

### Content Break Down

Content Type	Bytes from CDN	Bytes from Peers	Total Bytes	Device C...
Feature and Flight Updates	0 Bytes	0 Bytes	0 TB	0
Quality Updates	328.29 GB	1.52 TB	1.84 TB	3160
Office	82.92 GB	24.84 GB	0.11 TB	488
Driver Updates	8.66 GB	3.78 GB	0.01 TB	329
Other	1.29 TB	961.61 GB	2.23 TB	3394
Apps	84.71 GB	99.09 GB	0.18 TB	3275

### Content Types - By Source



### Bandwidth Savings - Optimal

Your delivery optimization settings are working very well, and you have significant volumes of traffic using peer to peer distribution.

#### Bandwidth Savings

2.58 TB

#### CDN Bandwidth

1.79 TB

### Update Sources Trend



### Update Sources Trend Last 7 days





# MEMUG Scotland

**MORE DEMO TIME...**



**PATCH**  
MY PC



# USEFUL RESOURCES

- **Azure Monitor Community (GitHub)**

- [GitHub - microsoft/AzureMonitorCommunity: An open repo for Azure Monitor queries, workbooks, alerts and more](#)

- **MSEndpointMgr**

- [Windows Update Compliance Workbook Community Edition – MSEndpointMgr](#)
- [Intune BIOS Update Compliance Reporting – MSEndpointMgr](#)
- [CloudLAPS Analytics and Monitoring – MSEndpointMgr](#)
- [Log Analytics & AppLocker - Better Together – MSEndpointMgr](#)
- [Delivery Optimization Configuration & Monitoring – MSEndpointMgr](#)

# USEFUL RESOURCES

- **Peter van der Woude**

- [Enhance Update Compliance with a custom Workbook in Microsoft Endpoint Manager admin center – All about Microsoft Endpoint Manager \(petervanderwoude.nl\)](https://petervanderwoude.nl)

- **Damian Van Robaeys**

- [Intune reporting with Log Analytics: list local admin accounts on your devices and who added them | Syst & Deploy \(systanddeploy.com\)](https://systanddeploy.com)
- [Intune reporting with Log Analytics: analyze disk size to see what's taking up place | Syst & Deploy \(systanddeploy.com\)](https://systanddeploy.com)

# FIN.

## **Beyond Native Reporting! – It's a wrap**

I hope you found this informative! Next up..



Can you please answer the second question now!

