

## EVIDEN LANDING ZONES FOR AZURE CLOUD CORE DASHBOARD AND WORKBOOK INSTRUCTION MANUAL

**Author(s)** : **Klaas Jan de Jager**  
**Version** : **1.0**  
**Status** : **Final**  
**Source** : **Eviden Landing Zones for Azure**  
**Document date** : **27 November 2023**  
**Number of pages** : **50**

## Contents

List of changes.....	4
1. Eviden Landing Zones for Azure Cloud Core Reporting Dashboard .....	5
2. IAM Reports.....	8
2.1 IAM Reports – Tenant Users.....	8
2.2 IAM Reports - Tenant Groups.....	9
2.3 IAM Reports – Roles and Admins.....	11
2.4 IAM Reports – Subscription Roles.....	12
2.5 IAM Reports – App Registrations.....	13
3. Help + Support.....	15
4. Operational Reports .....	16
5. Policies Reports.....	17
5.1 Policy Assignments.....	17
5.2 Policy Compliance report.....	18
6. Financial Reports.....	20
6.1 Cost Management.....	20
6.2 Cost Advisor .....	22
7. Offline Reports.....	23
7.1 Overview of resources with EvidenManaged tag is True.....	25
7.2 Virtual Machine overview Eviden management Tags and Patching status... ..	26
7.3 Virtual Machine availability monthly overview.....	26
7.4 PAAS services with EvidenManaged tag is True.....	26
8. Azure Consumption workbook .....	28
9. Security Log Exception workbook.....	29
10. Compliance report.....	31
11. Orphan resources workbook.....	33
11.1 The orphaned resource overview blade .....	33
11.2 A detailed blade per orphaned resource type.....	34
12. PIM Role Assignments workbook.....	36
13. Log Analytics Workspace workbook.....	38
13.1 Log Analytics Workspace Configuration Overview.....	38

13.2 Log Analytics Workspace Workloads.....	39
13.2.1    Health Overview .....	39
13.2.2    Usage Overview .....	40
14. Maintenance workbook.....	42
15. Virtual WAN workbook.....	43
15.1 Overview blade.....	43
15.2 VPN Gateways blade.....	46
15.3 VPN Sites blade .....	47
15.4 ExpressRoute Gateways blade.....	49

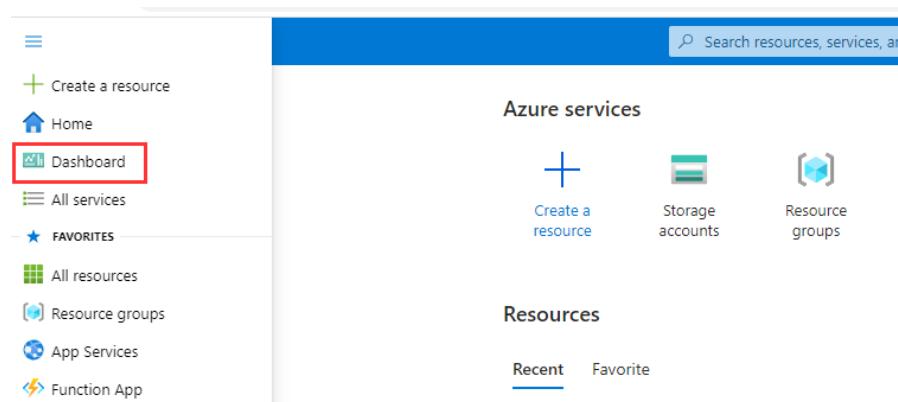
## List of changes

Version	Date	Description	Author(s)
0.9	22-08-2023	Draft Eviden version	K.J. de Jager
1.0	31-10-2023	Initial Eviden version	K.J. de Jager

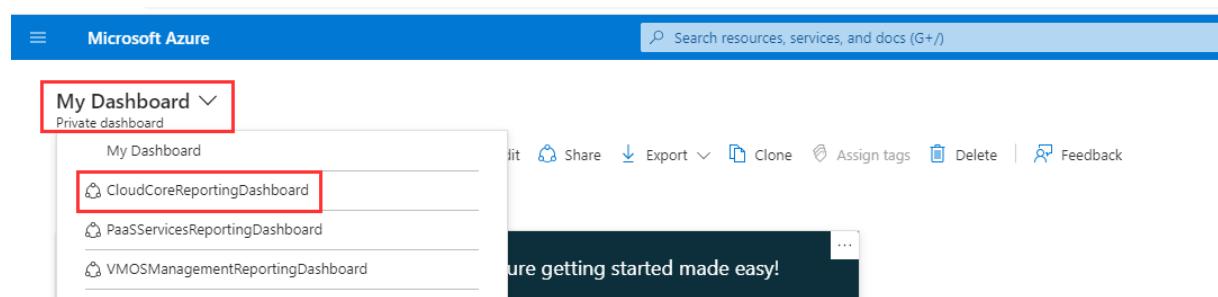
## 1. Eviden Landing Zones for Azure Cloud Core Reporting Dashboard

This dashboard is an entry point that guides you to get most of the insights of your cloud environment. The dashboard consists of several tiles that direct you to the concerning Azure Blade, Workbook, or Storage Account Container. These tiles are grouped by category namely, IAM, Operational, Policy, and Financial. You can scroll up and down through the dashboard to see all groups and tiles. In the following paragraphs all tiles and workbooks will be shortly described.

To access the shared dashboard simply click on the menu on the top left in the portal. By default, “Dashboard” button is set on the top, see image below.



This should directly send you to the correct dashboard. If this is not the case, change the dashboard add the left top corner by clicking on the dashboard title and select CloudCoreReportingDashboard, see image below.



**Note:** In case the environment has been upgraded from a previous release, it is possible that 'old dashboard names' may still appear in this overview. Once one of these is selected, an error message should be shown, and after that, the dashboard will disappear from the dropdown menu.

The Cloud Core Reporting dashboard, as in the picture below, now appears:

**CloudCoreReportingDashboard** Shared dashboard

+ Create ⚡ Upload ⚡ Refresh ↗ Full screen | Edit Manage sharing Export Clone Assign tags Delete Feedback

Auto refresh : Off UTC Time : Past 24 hours X

IAM Reports

- Tenant Users
- Tenant Groups
- Roles and Admins
- App Registrations
- Subscription Roles
- Offline Reports

Maintenance Report Azure Monitor

Orphan resources Azure Monitor

Log Analytics Works... Azure Monitor

PIM Role Assignments Azure Monitor

Virtual WAN Azure Monitor

Help + Support Placeholder

Ticketing

Operational Reports

- Incident Report
- Change Report

Policy Reports

- Pol. Assignments
- Pol. Compliance

Financial Reports

- Cost Management
- Cost Advisor

Compliance Report

Eviden Landing Zones for Azure - Cloud Core Reporting dashboard Release 2.3 (Release Notes)

Getting Started with Cloud Core Reporting

First time using this dashboard? Click the image below to get started.

In the text under the **Eviden Logo [1]**, you will find the version of Eviden Landing Zones for Azure that is deployed.

At the next line you find a link to the *Release notes* that will redirect to the Eviden Landing Zones for Azure release notes page.

The tile “**Getting Started with Cloud Core Reporting**” [2] redirects you to the up-to-date version of the getting started manual (this document) that is part of the release as displayed underneath the logo.

In the following paragraphs all other tiles and workbooks that are part of this dashboard will be shortly described.

## 2. IAM Reports

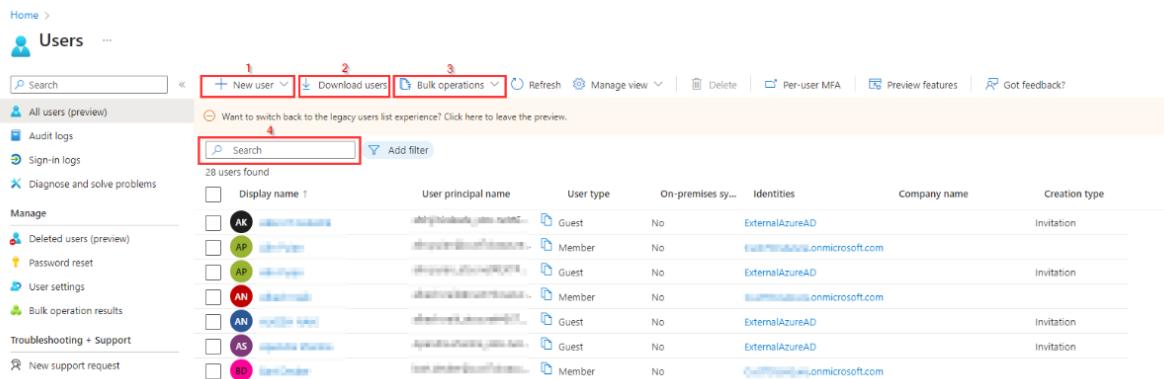
IAM Reports is a section in the dashboard that consists of 5 tiles that contains a link to redirect you to an Azure blade where the respective reports can be found:

- Tenant Users: Customer Tenant Azure AD Users
- Tenant Groups: Customer Tenant Azure AD Groups
- Roles and Admins: Customer Tenant Azure AD Roles (such as global admin or many others: Users or Groups are added to Roles to be granted AD-level rights)
- App Registrations: Customer Tenant Azure AD App Registrations to create registrations for applications and assign permissions accordingly.
- Subscription Roles: Per customer subscription IAM Roles (such as subscription owner, contributor, etc...: Users or Groups are added to roles to be granted subscription-level rights)

These reports provide details on identity and access management in Azure, like users, groups, roles and app registrations defined within the customer subscription(s). For this report it is key to have a clear overview of the users and roles. For a detailed description about Azure AD, check this [link](#).

### 2.1 IAM Reports – Tenant Users

The Tenant Users tile in the dashboard redirects you to the Azure Active Directory Users blade in the customer environment:



Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
AK	ak@tenant.onmicrosoft.com	Guest	No	ExternalAzureAD		Invitation
AP	ap@tenant.onmicrosoft.com	Member	No	ExternalAzureAD@onmicrosoft.com		Invitation
AP	ap@tenant.onmicrosoft.com	Guest	No	ExternalAzureAD		Invitation
AN	an@tenant.onmicrosoft.com	Member	No	ExternalAzureAD@onmicrosoft.com		Invitation
AN	an@tenant.onmicrosoft.com	Guest	No	ExternalAzureAD		Invitation
AS	as@tenant.onmicrosoft.com	Guest	No	ExternalAzureAD		Invitation
BS	bs@tenant.onmicrosoft.com	Member	No	ExternalAzureAD@onmicrosoft.com		Invitation

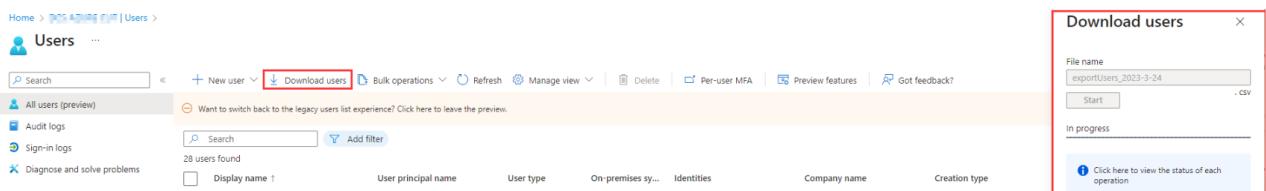
In the ‘users blade’ the Azure active directory users can be managed like creating a **New user [1]**, **Download users overview [2]** or perform **Bulk operations [3]** on users.

**New User[1]** has two options:

- *Create new user:* Create a new internal user in your organisation.
- *Invite external user:* Invite an external user to collaborate with your organisation.

For more information about both options, check this [link](#)

**Download users [2]** is a good feature to create a report on all users if there are a lot of users created already. By selecting Download users a window is opened at the right top of the blade:



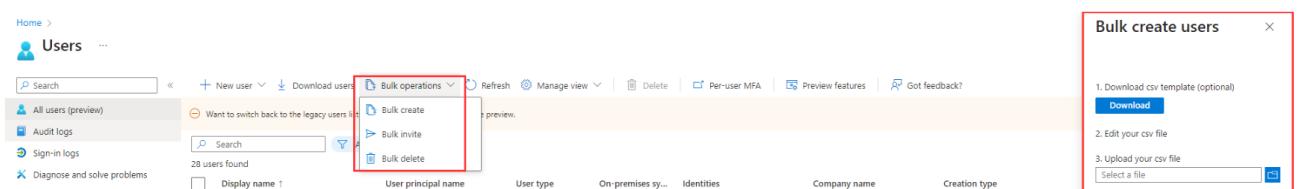
The screenshot shows the 'Users' blade in the Azure portal. At the top, there's a search bar and several navigation links like 'New user', 'Download users', 'Bulk operations', etc. Below the search bar, there's a list of users with columns for 'Display name', 'User principal name', 'User type', etc. On the right, a 'Download users' dialog box is open, showing a file name 'exportUsers\_2023-3-24.csv' and a 'Start' button. The status says 'In progress'. There's also a link 'Click here to view the status of each operation'.

In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded, you will get the option to download the file.

**Bulk operations [3]** is a nice feature to create a lot of users at once. This is especially handy right after the customer environment is deployed and all customer users need to be added to Azure AD.

This feature can also be used for **Bulk invite** or **Bulk delete** of users.

For the bulk options a **CSV template** need to be created and uploaded to Azure:



The screenshot shows the 'Users' blade with the 'Bulk operations' dropdown menu open, showing options like 'Bulk create', 'Bulk invite', and 'Bulk delete'. To the right, a 'Bulk create users' dialog box is open, containing steps: 1. Download csv template (optional) with a 'Download' button, 2. Edit your csv file, and 3. Upload your csv file with a 'Select a file' input field.

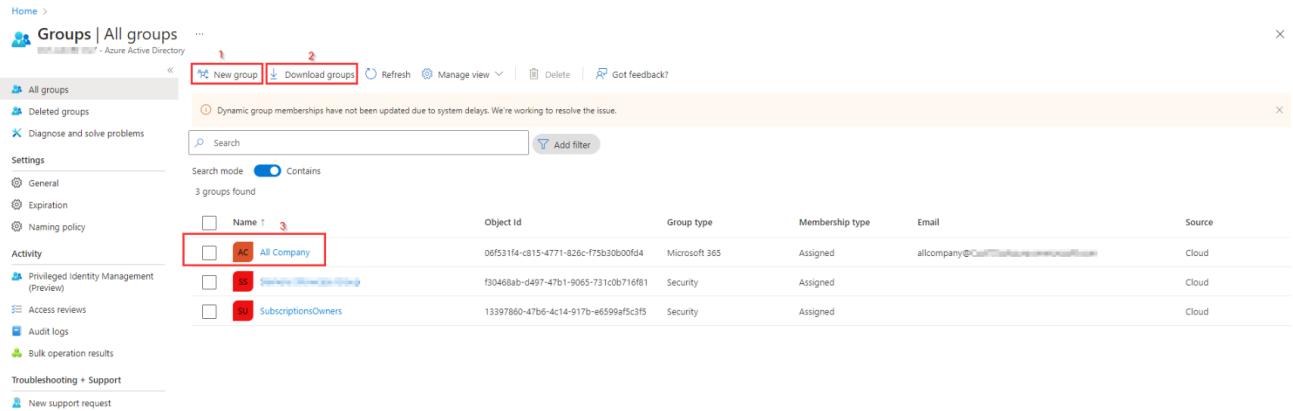
More information about bulk operations can be found here:

- [Create users in bulk](#)
- [Delete users in bulk](#)

**Bulk import service limits:** Each bulk activity to create users can run for up to one hour. This enables bulk creation of at least 50,000 users.

## 2.2 IAM Reports - Tenant Groups

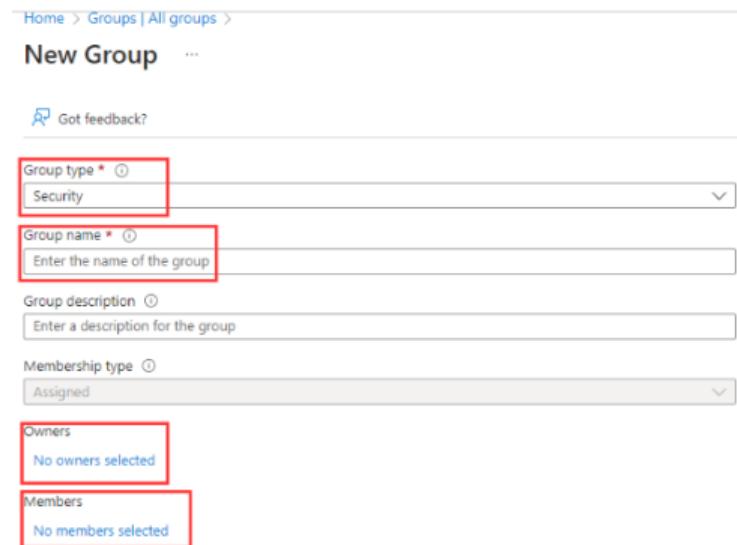
The Tenant Groups tile in the dashboard redirects you to the Azure Active Directory Groups blade in the customer environment:



The screenshot shows the 'Groups | All groups' blade in the Azure Active Directory portal. At the top, there are two red boxes: [1] 'New group' and [2] 'Download groups'. Below these are buttons for 'Refresh', 'Manage view', 'Delete', and 'Got feedback?'. A message states: 'Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.' A search bar and filter button ('Add filter') are also present. The main area displays a table of groups with columns: Name, Object Id, Group type, Membership type, Email, and Source. Three groups are listed: 'All Company' (Microsoft 365, Assigned, allcompany@contoso.com, Cloud), 'SubscriptionsOwners' (Security, Assigned, SubscriptionsOwners, Cloud), and 'SubscriptionsReviewers' (Security, Assigned, SubscriptionsReviewers, Cloud). A sidebar on the left includes sections like 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings', 'Activity', 'Access reviews', 'Audit logs', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'.

In this groups blade the Azure active directory groups can be managed like creating a **New group [1]** and **Download groups overview [2]**.

**New group [1]** opens a separate window to create a new group by selecting the Group type (Security or Microsoft 365), the Groups name and assign Owners and Members to the new group.

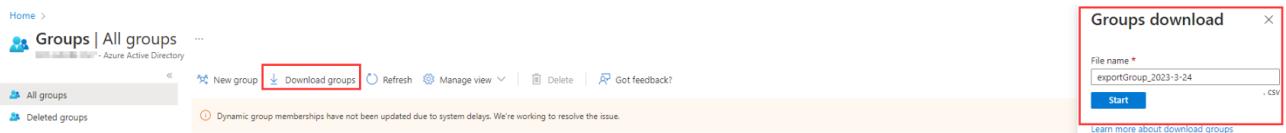


The screenshot shows the 'New Group' dialog. It includes fields for 'Group type \*' (Security), 'Group name \*' (Enter the name of the group), 'Group description' (Enter a description for the group), 'Membership type' (Assigned), and sections for 'Owners' (No owners selected) and 'Members' (No members selected). A 'Got feedback?' link is also present.

By selecting an **existing group [3]** this groups can be managed, like adding users to or removing users from this group or add/remove Azure role assignments.

For more information about the creation of groups or manage the groups check this [link](#).

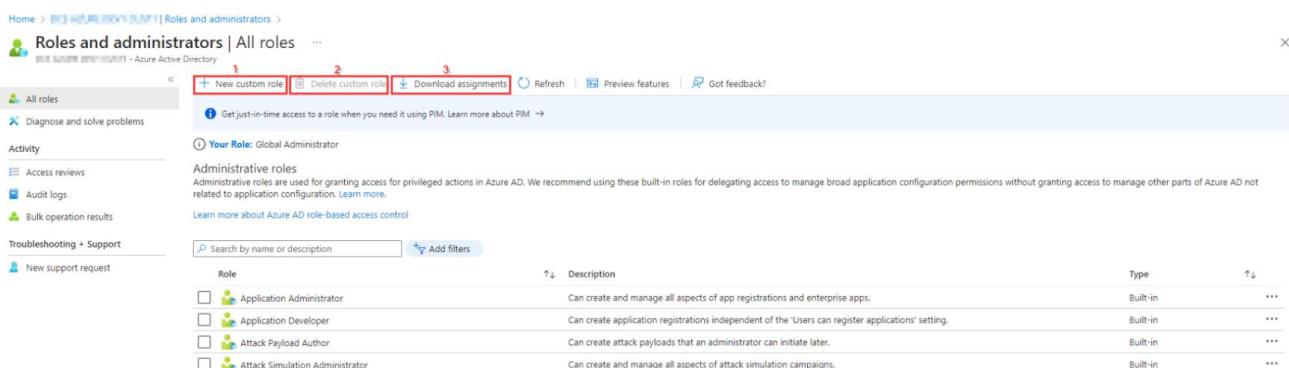
**Download groups [2]** is a good feature to create a report on all groups if there are a lot of groups created already. By selecting **Download groups** a windows is opened at the right top of the blade:



In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded, you will get the option to download the file.

## 2.3 IAM Reports – Roles and Admins

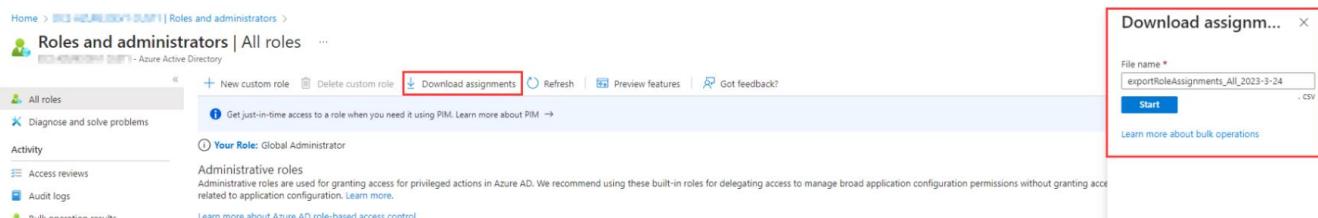
The Roles and Admins tile in the dashboard redirects you to the Azure Active Directory Roles and Admins blade in the customer environment:



Role	Description	Type
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	Built-in
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in

Administrative roles are used for granting access for privileged actions in Azure AD. In this blade you can create a **New custom role[1]**, **Delete a custom role [2]** or **Download assignments [3]**.

**Download assignments [3]** is a good feature to create a report on role assignments. By selecting **Download assignments** a windows is opened at the right top of the blade:



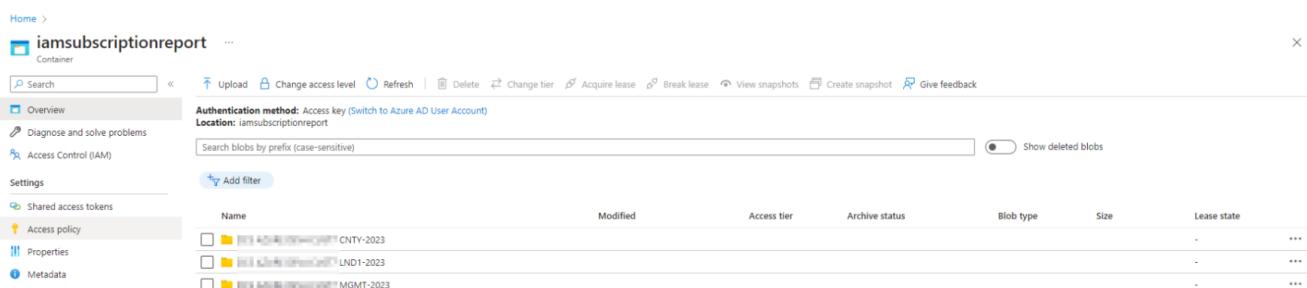
In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded you will get the option to download the file.

For more information about role-based access control check this [link](#).

## 2.4 IAM Reports – Subscription Roles

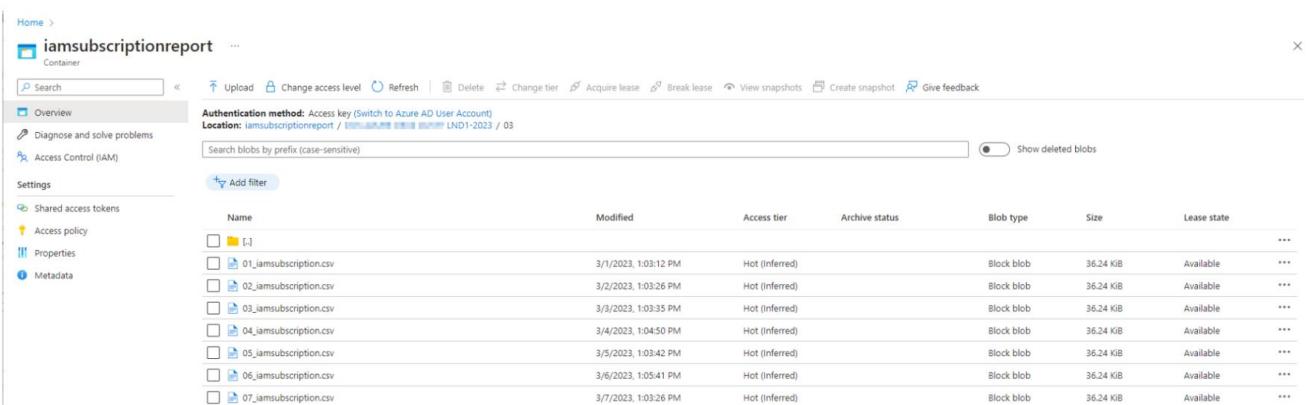
The **Subscription Roles** tile redirects you to a **Storage container** where reports are saved that are created every 12 hours using the **Get-AzureSubscriptionRolesForReporting runbook**. For each day only one report is preserved.

The contents of this iamsubscriptionreport container will look like this.



Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
CNTY-2023					-	---
LND1-2023					-	---
MGMT-2023					-	---

The **Subscription Roles reports** are reports that contains Subscription Role assignment information and are **created based on a schedule** and saved in **CSV file format**. The reports are saved **per subscription per year in a separate folder**. In every subscription folder you find folders with the numbers of the month. the contents of a monthly folder will look like this:

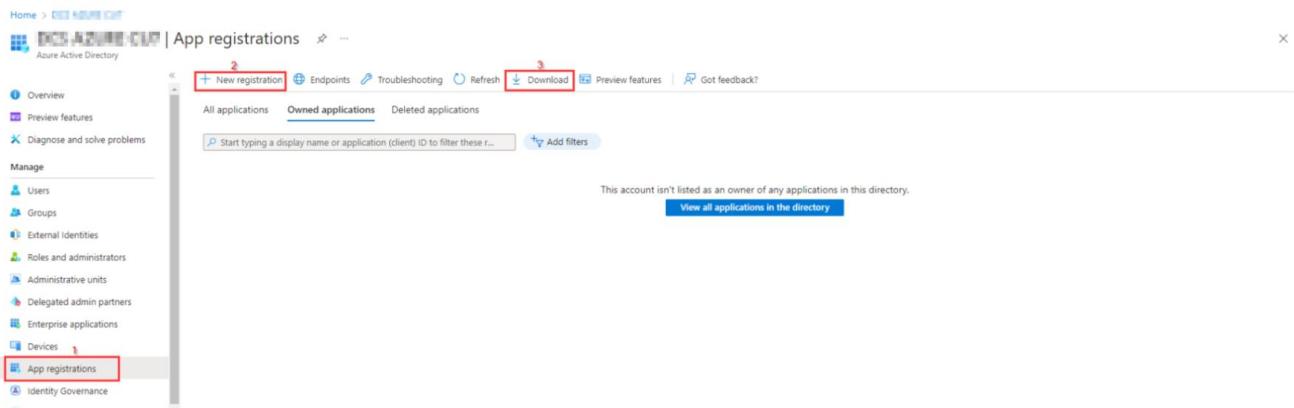


Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
01_iamsubscription.csv	3/1/2023, 1:03:12 PM	Hot (Inferred)		Block blob	36.24 kB	Available
02_iamsubscription.csv	3/2/2023, 1:03:26 PM	Hot (Inferred)		Block blob	36.24 kB	Available
03_iamsubscription.csv	3/3/2023, 1:03:35 PM	Hot (Inferred)		Block blob	36.24 kB	Available
04_iamsubscription.csv	3/4/2023, 1:04:50 PM	Hot (Inferred)		Block blob	36.24 kB	Available
05_iamsubscription.csv	3/5/2023, 1:03:42 PM	Hot (Inferred)		Block blob	36.24 kB	Available
06_iamsubscription.csv	3/6/2023, 1:05:41 PM	Hot (Inferred)		Block blob	36.24 kB	Available
07_iamsubscription.csv	3/7/2023, 1:03:26 PM	Hot (Inferred)		Block blob	36.24 kB	Available

These reports can be used for monthly management reporting or for later reference.

## 2.5 IAM Reports – App Registrations

The App Registrations tile in the dashboard redirects you to the Azure Active Directory **App Registrations blade [1]** in the customer environment:



In this blade **New registrations [2]** for applications can be added to Azure Active Directory to establish a trust relationship between your application and the identity provider, the Microsoft identity platform. For more information about registering an application, check this [link](#).

The **Download [3]** option enables you to create and download a CSV file with *All applications* or *Owned applications*.

Download app registrations ×

Select which app list you would like to download, and set the name for your new file. The download format for the app registrations will be based on the Microsoft Graph Application schema. [Learn more](#)

App list selection

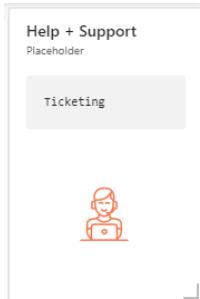
All applications  
 Owned applications

File name

AppRegistrationList .csv

Download

### 3. Help + Support

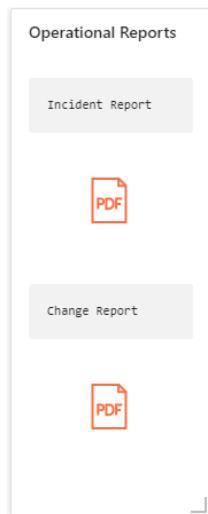


The Help + Support section has only one tile at this moment that is a placeholder that will redirect to the home blade of the Azure portal.

This section is meant to provide tile for Help and Support, like a tile to a ticketing service. As this is not available yet the Ticketing tile redirects to the Azure Portal.

In the future this link can be changed to redirect to a ticketing system or other means to provide help and support.

## 4. Operational Reports



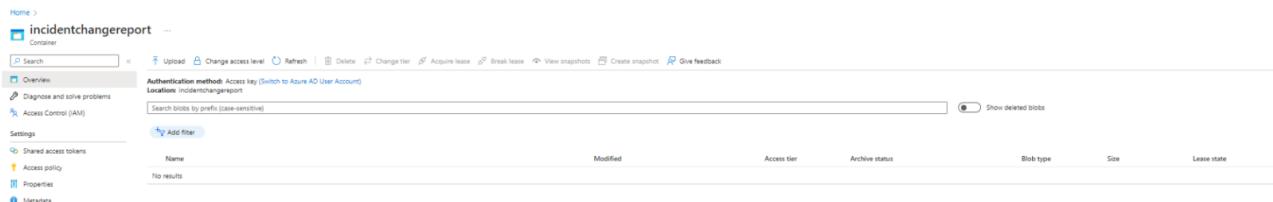
Operational Reports is a separate section in the dashboard that consists of 2 tiles that both contains a link to redirect you to a separate Storage Account container where the respective reports can be found:

Incident Report: Links to the incidentchangereport container at the storage account for reporting.

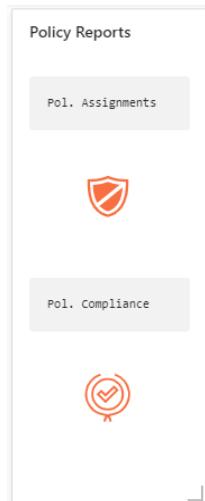
Change Report: Links to the incidentchangereport container at the storage account for reporting.

In the incidentchangereport container, where both links redirect to, reports, extracted from ITSM Service Now in PDF format should be manually uploaded once per month. The name should have a prefix of year-month-filename.

By default, this container will be empty:



## 5. Policies Reports



Policies Reports is a section in the dashboard that consists of 2 tiles that both contains a link to redirect you to a Azure blade where the respective reports can be found:

- Policy Assignments: Links to the Policy Assignments blade in Azure
- Policy Compliance: Links to the Policy Compliance blade in Azure

These reports provide details on active policies defined within the customer subscription(s). One of the largest benefits of Azure Policy is the insight and controls it provides over resources in a subscription or management group of subscriptions. For more information on Azure Policies, check this [link](#).

### 5.1 Policy Assignments

The policy assignments blade in Azure provides an overview of all assigned policies and initiatives for the selected **Scope [1]**. By default all subscriptions are selected in the Scope filter, but it is possible to select one or more specific subscriptions to create an overview on.

With the **Definition type [2]** filter it is possible to select on '*Initiative*', '*Policy*' or on '*All definition types*'.

Scope	Type
[Redacted]	Policy
[Redacted]	Initiative

The **Search filter [3]** makes it possible to filter on a keyword are name in Initiative or Policy.

Apart from the overview it's also possible to **Assign policies [4]** or **Assign Initiatives [5]** in this Policy Assignments blade.

For more information about assigning policies, check this [link](#).

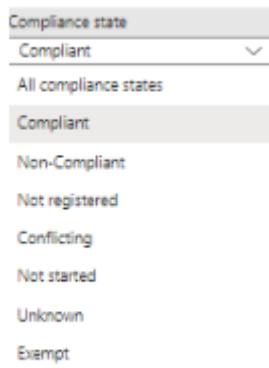
## 5.2 Policy Compliance report

The policy compliance blade in Azure provides an overview of the compliance state of policies and initiatives for the selected **Scope [1]**. By default all subscriptions are selected in the Scope filter, but it is possible to select one or more specific subscriptions to create an overview on.

With the **Type [2]** filter it is possible to select on '*Initiative*', '*Policy*' or on '*All definition types*'. The Compliance state filter [3]

The screenshot shows the Azure Policy | Compliance blade. At the top, there are filters for Scope (4 selected), Type (All definition types), and Compliance state (Compliant). Below these are summary metrics: Overall resource compliance (24%, 157 out of 653), Resources by compliance state (653 Compliant, 496 Non-compliant), Non-compliant initiatives (25 out of 137), and Non-compliant policies (343 out of 7406). A donut chart visualizes the compliance status. The main area displays a table of non-compliant resources, each with a preview icon, name, scope, compliance state, resource compliance percentage, and non-compliant resources count. The table includes columns for Name, Scope, Compliance state, Resource compliance, Non-Compliant Resources, and Non-compliant policies.

The **Compliance state filter [3]** provides the option to filter on one of the following Compliance states:

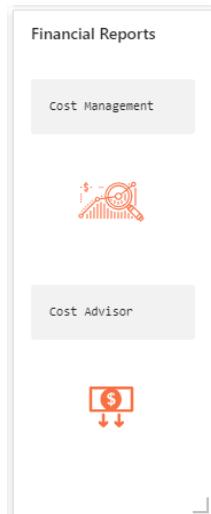


The **Search filter [4]** makes it possible to filter on a keyword are name in Initiative or Policy.

Apart from the overview it's also possible to **Assign policies [5]** or **Assign Initiatives [6]** in this Policy Assignments blade.

For more information about assigning policies, check this [link](#).

## 6. Financial Reports



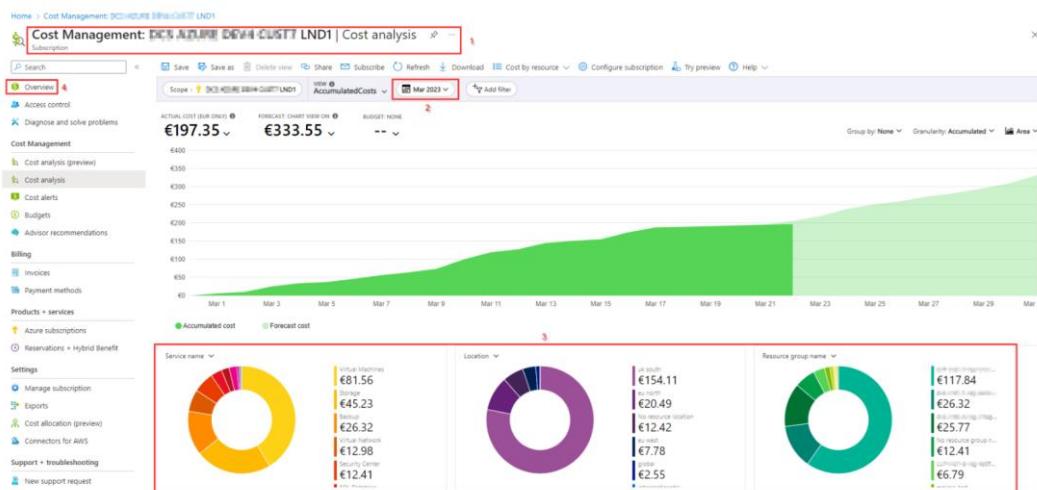
Financial reports is a separate section in the dashboard that consists of 2 tiles that both contains a link to redirect you to an Azure blade that contains information about:

- Cost Management: This tile redirects to the Cost Analysis blade in Azure Cost Management.
- Cost Advisor: This tile redirects to the Advisor recommendations blade in Azure Cost Management.

These reports provide details on the charges attracted by services in use in the customer subscription(s). To do cost analysis an Enterprise subscription is needed. With a CSP subscription cost analysis is not possible.

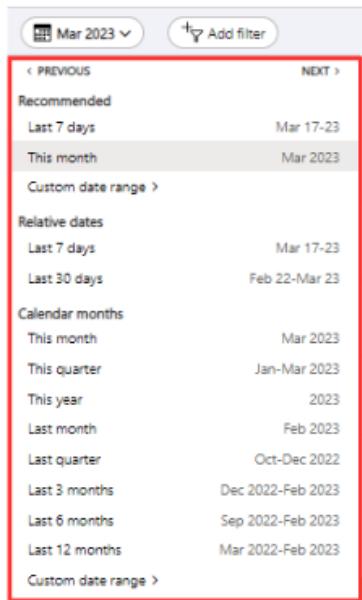
### 6.1 Cost Management

By selecting the Cost Management tile you are redirected to the following blade in Azure:



At the top of this **blade [1]** you find the subscription for which the Cost Management blade is visible.

Cost Management is visible on a per subscription overview. The overview provides the actual cost and a forecast for the selected **time range [2]**. Possible time ranges are:



where **Custom date range** can be a range within the last 2 years.

At the bottom of the blade there are **3 pie charts [3]** with more detailed cost information on specific resources, services or tags that can be selected in the filters on top of the pie chart.

To change the scope for cost management, select **Overview [4]** at the left of this blade and click on **(change)** to select another subscription or a resource group within a subscription.

The screenshot shows the Azure Cost Management blade on the left and a 'Select scope' dialog box on the right. The blade includes a sidebar with navigation links like Home, Overview, Access control, and Diagnose and solve problems. The main area displays 'Analyze and optimize cloud costs' with three cards: 'Setup your account', 'Report on and analyze trends', and 'Control and implement'. The 'Select scope' dialog shows a list of scopes: CNTV, LND1 (selected), and LND2. There are buttons for 'Select' and 'Cancel' at the bottom.

For more information about this Cost Management blade, check this [link](#).

## 6.2 Cost Advisor

By selecting the Cost Advisor tile you are redirected to the **Advisor recommendations blade [1]** in Azure:

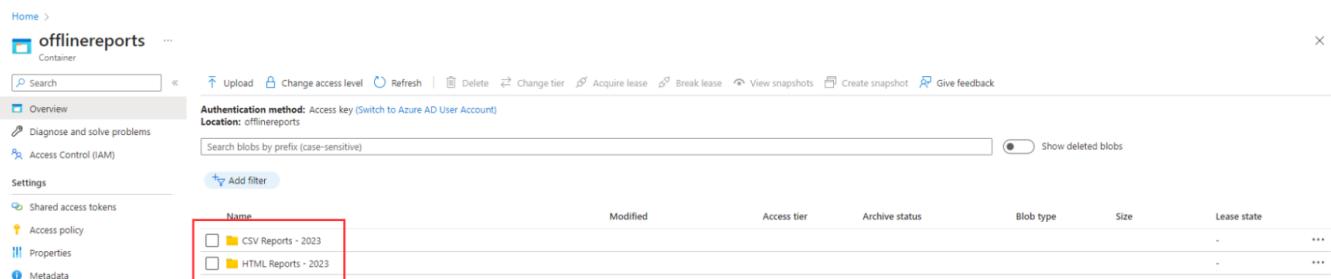
Based on the selection in the **filters [2]** at the top of this blade there are Advisor recommendations shown, if any.

In this blade it is possible to **Create alerts [3]** or **Create recommendation digests [4]**.

More information about **cost recommendations [5]** can be found by selecting this [link](#)

## 7. Offline Reports

The Offline Reports tile redirects you to the **offlinereports** container where the offline reports are created in both CSV and HTML format, both in a separate folder for each year.

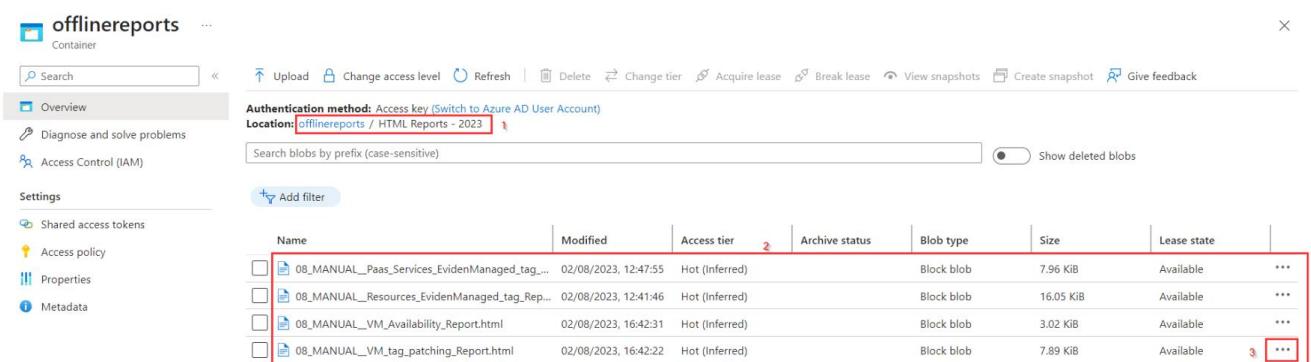


Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
CSV Reports - 2023					-	---
HTML Reports - 2023					-	---

By default, the following reports can be found, that are created at the end of each month:

- **Resources with Eviden Managed tag:** provides an overview on a monthly basis with all resources that has the **EvidenManaged** tag set with value "True".
- **VM tag and patching:** provides an overview on a monthly basis with the patch settings and values for the Eviden tags.
- **VM availability:** provides an overview on a monthly basis with the availability of each VM.
- **PAAS services with EvidenManaged Tag:** provides an overview on a monthly basis with the PAAS Services that has the EvidenManaged tag set to 'True'

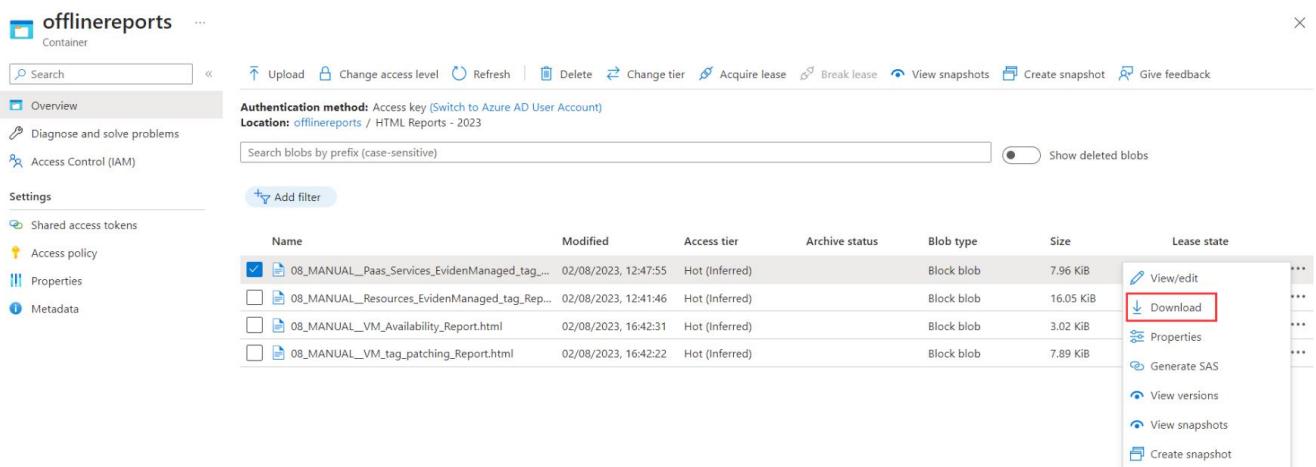
The reports can be found by selecting the folder for the CSV or HTML, like for example "**HTML Report - 2023**" [1]:



Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
08_MANUAL_PaaS_Services_EvidenManaged_tag_Report.html	02/08/2023, 12:47:55	Hot (Inferred)		Block blob	7.96 KiB	Available
08_MANUAL_Resources_EvidenManaged_tag_Report.html	02/08/2023, 12:41:46	Hot (Inferred)		Block blob	16.05 KiB	Available
08_MANUAL_VM_Availability_Report.html	02/08/2023, 16:42:31	Hot (Inferred)		Block blob	3.02 KiB	Available
08_MANUAL_VM_tag_patching_Report.html	02/08/2023, 16:42:22	Hot (Inferred)		Block blob	7.89 KiB	Available

In this folder for 2023 a report is created each month starting with the number of the **month [8]**. The text 'MANUAL' between underscores after the number of the month means that the runbook that created the offline report is manually started. When the report is created by a schedule, as is usually the case for a monthly report, this text omits.

By selecting the **three-dots [3]** at the right of the file name a menu is opened where the file can be downloaded and opened (for an HTML file) or imported in excel (for a CSV):



Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
08_MANUAL_PaaS_Services_EvidenManaged_tag_Report.html	02/08/2023, 12:47:55	Hot (Inferred)		Block blob	7.96 KiB	
08_MANUAL_Resources_EvidenManaged_tag_Report.html	02/08/2023, 12:41:46	Hot (Inferred)		Block blob	16.05 KiB	
08_MANUAL_VM_Availability_Report.html	02/08/2023, 16:42:31	Hot (Inferred)		Block blob	3.02 KiB	
08_MANUAL_VM_tag_patching_Report.html	02/08/2023, 16:42:22	Hot (Inferred)		Block blob	7.89 KiB	

The following reports will be available for download in both CSV and HTML format (where XX = # Month):

### **Cloud Core reports:**

- *XX\_Resources\_EvidenManaged\_tag\_Report*: Overview of resources with EvidenManaged tag set to True.

### **OS-management reports:**

- *XX\_VM\_tag\_patching\_Report*: Virtual Machine overview Eviden management Tags and Patching status.
- *XX\_VM\_Availability\_Report*: Virtual Machine availability monthly overview.

### **PAAS Services Management reports:**

- *XX\_Paas\_Services\_EvidenManaged\_tag\_Report*: PAAS services with EvidenManaged tag set to True overview.

## 7.1 Overview of resources with EvidenManaged tag is True.

This offline report provides an overview of all resources in the customer environment that has the Eviden Managed tag set to True.

In HTML the report will look like this:

### Resources with EvidenManaged tag is "true" monthly Report 2023/08

RESOURCE NAME	TYPE	SUBSCRIPTION	RESOURCE GROUP
0c60cb2f-f15e-5e70-94f4-14e02079e21b	microsoft.insights/workbooks	MGMT	
15e69b12-3ac0-508d-b019-8bc5a9520780	microsoft.insights/workbooks	MGMT	
2333675c-d0c5-5ccc-9f7e-9aad4b9edb4c	microsoft.insights/workbooks	MGMT	
2ed365f1-90de-5414-9f02-8bc499255123	microsoft.insights/workbooks	MGMT	
32d8bcb4-b953-5fe6-bd18-6f0a2f025883	microsoft.insights/workbooks	MGMT	
35cf9b8c-0d28-5ebd-99a6-1c436bd16ba8	microsoft.insights/workbooks	MGMT	
36e78b63-ed19-5ade-957f-c73436943484	microsoft.insights/workbooks	MGMT	
4180b998-4a2f-54ff-afbb-0006a85c97a8	microsoft.insights/workbooks	MGMT	
43e1dff3-6814-523f-9d28-cedbf6a8c3a0	microsoft.insights/workbooks	MGMT	
4e37c44c-477d-5b81-964e-1bd954417a31	microsoft.insights/workbooks	MGMT	
546ed212-ee4a-5b5a-8f33-25d08c250ae2	microsoft.insights/workbooks	MGMT	
58feb3ed-02b4-58c7-8250-08b802445319	microsoft.insights/workbooks	MGMT	
5935553c-3279-57d8-8d2c-8d2ef020ae9c	microsoft.insights/workbooks	MGMT	
5cd07614-bfef-50f1-80ff-1a5fd03a5049	microsoft.insights/workbooks	MGMT	
686618ba-9479-574b-a0a2-e4acb272f662	microsoft.insights/workbooks	MGMT	
6ffd986a-774d-5086-8547-e348f26caab5	microsoft.insights/workbooks	MGMT	
75b08639-dba6-5888-a34e-4aefbf720fa	microsoft.insights/workbooks	MGMT	
7c4a98e9-d92f-5453-960f-b32ede31320b	microsoft.insights/workbooks	MGMT	
847edb8f-9151-5157-85b3-95e5dfc5b715	microsoft.insights/workbooks	MGMT	
8fde7685-2a57-53a2-bfe9-36ac845be275	microsoft.insights/workbooks	MGMT	
9039b0db-3c3a-516d-a0df-c52bc3e54b80	microsoft.insights/workbooks	MGMT	
98d00e5b-54bd-5908-b0e7-48f2a3982a29	microsoft.insights/workbooks	MGMT	

### Known Issue's

If the query doesn't find any resource (No resources with EvidenManaged tag set to True are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.2 Virtual Machine overview Eviden management Tags and Patching status

This offline report provides an overview of Virtual Machines in the customer environment and the tags that are used for Eviden Management. This report also provides an overview if the virtual machine is patched.

In HTML the report will look like this:

VM Tagging and Patching monthly Report 2023/08

VIRTUAL MACHINE	RESOURCE GROUP	SUBSCRIPTION	PATCHSTATE	EVIDENPATCHING	EVIDENOSVERSION	EVIDENMANAGED	EVIDENANTIMALWARE	EVIDENCOMPLIANCE	EVIDENBACKUP	EVIDENENCRYPTION
alikeshvmfordevelop	alikeshvmfordevelop	alikeshvmfordevelop	LND1 VM does not have the correct tags			False	False	False		False
lnvm01	lnvm01	lnvm01	LND2 VM is EvidenManaged but not in Patch Schedule	Linux-Dev		True	False	False		False
lnvm02	lnvm02	lnvm02	LND2 VM is EvidenManaged but not in Patch Schedule	Linux-Test		True	False	False		False
lnvm03	lnvm03	lnvm03	LND1 VM is EvidenManaged and in Patch Schedule	Linux-Dev	redhat 8.7	True	False	False	Gold	False
snowpatched001	snowpatched001	snowpatched001	LND1 VM does not have the correct tags			False	False	False		False
winvm01	winvm01	winvm01	LND1 VM is not EvidenManaged but in Patch Schedule	windows-dev		False	False	False	Silver	False
winvm03	winvm03	winvm03	LND2 VM is EvidenManaged but not in Patch Schedule	windows-dev		True	False	False	Gold	False
winvm06	winvm06	winvm06	LND1 VM is EvidenManaged and in Patch Schedule	windows-dev	Windows Server 2016 Datacenter	True	False	False		False
winvm07	winvm07	winvm07	LND1 VM does not have the correct tags			False	False	False		False

### Known Issue's

If the query doesn't find any resource (No VM's are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.3 Virtual Machine availability monthly overview

This offline report provides an overview of Virtual Machines in the customer environment with their availability over a month and if the virtual machine is managed by Eviden.

In HTML the report will look like this:

VM availability monthly Report 2023/08 for log analytics workspace: alikeshvmfordevelop-mgmt-t-loganalytics

VIRTUAL MACHINE	OPERATING SYSTEM	SUBSCRIPTION	RESOURCE GROUP	START TIME RANGE	END TIME RANGE	AVAILABILITY PERCENTAGE	TOTAL AVAILABLE HOURS	TOTAL HOURS	MANAGED BY EVIDEN
testfredaks01	Linux	alikeshvmfordevelop	LND1 alikeshvmfordevelop	23-08-01 [00:00:00]	23-08-01 [00:00:00]	45.0 %	18	40	VM testfredaks01 is deleted before end of the month

### Known Issue's

If a virtual machine is created within the reported month this is not mentioned in the report, but availability percentage during the month will be less than 100%. If the query doesn't find any resource (No VM's are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.4 PAAS services with EvidenManaged tag is True.

This offline report provides an overview of all PAAS Services in the customer environment with the status of the Eviden Managed tag.

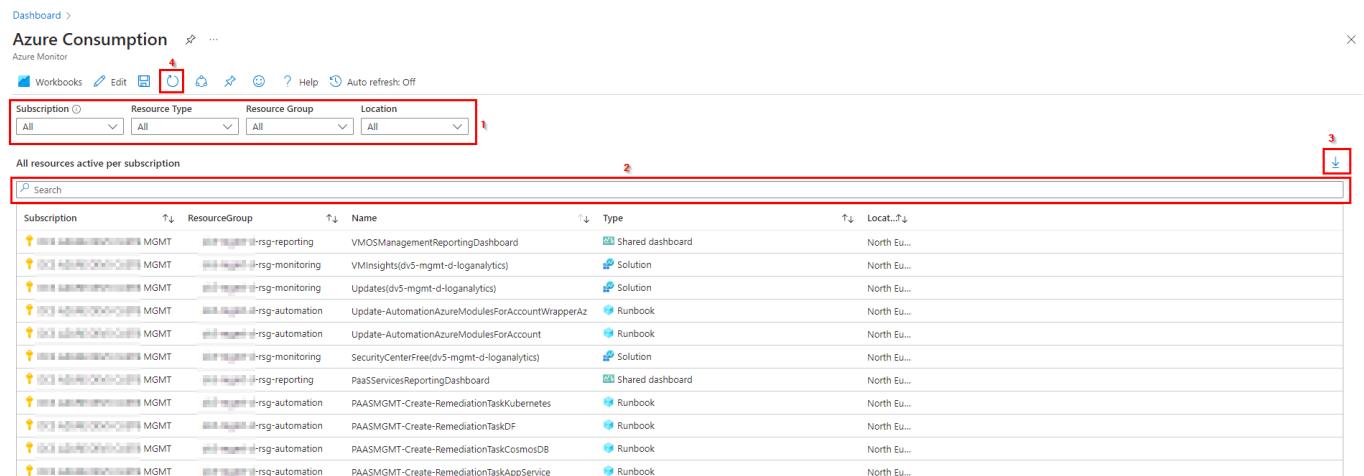
In HTML the report will look like this:

## PAAS Service overview with EvidenManaged State monthly Report 2023/08

NAME	TYPE	RESOURCE GROUP	SUBSCRIPTION	LOCATION	EVIDEN MANAGED
dv4-mgmt-t-logicapp-itsm-alerts	microsoft.logic/workflows	[REDACTED]	[REDACTED] MGMT	uksouth	False
Daily_atsix_start	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
Daily_atnine_stop	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
stsv2_vms_AutoStop	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
testcheck	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
stsv2_vms_Sequenced_start	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
stsv2_vms_Scheduled_start	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
stsv2_vms_Sequenced_stop	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
stsv2_vms_Scheduled_stop	microsoft.logic/workflows	[REDACTED]	[REDACTED] LND1	westeurope	False
dv4-mgmt-t-logicapp-itsm-cmdb	microsoft.logic/workflows	[REDACTED]	[REDACTED] MGMT	uksouth	False
bbd-hrut-d-functionapp-billing	microsoft.web/sites	[REDACTED]	[REDACTED] MGMT	westeurope	False
dv4-mgmt-t-functionapp-ostagging	microsoft.web/sites	[REDACTED]	[REDACTED] MGMT	uksouth	False
dv4-mgmt-t-functionapp-billing	microsoft.web/sites	[REDACTED]	[REDACTED] MGMT	uksouth	False
startstopv2testcheck	microsoft.web/sites	[REDACTED]	[REDACTED] LND1	westeurope	False
dv4-mgmt-t-functionapp-itsm-pwsh	microsoft.web/sites	[REDACTED]	[REDACTED] MGMT	uksouth	False
startstoppocama347xe4b42w	microsoft.web/sites	[REDACTED]	[REDACTED] LND1	westeurope	False

## 8. Azure Consumption workbook

The Azure Consumption report is used to provide an overview of all Azure services in use in customer subscription(s) managed by Eviden.



The screenshot shows the Azure Consumption workbook interface. At the top, there are four filter dropdowns: Subscription (All), Resource Type (All), Resource Group (All), and Location (All). A red box [1] highlights the Resource Type filter. Below the filters is a search bar [2] containing the text 'Search'. A red box [3] highlights the 'Export' button at the top right of the main table area. The main table lists various Azure resources, including dashboards, solutions, runbooks, and automation modules, categorized by subscription, resource group, name, type, and location. A red box [4] highlights the refresh icon at the top left of the table.

In the top part the report provides several **filters [1]** to select the resources to report on for a specific Subscription, Resource Type, Resource Group or Location. This way the filters at the top of the report can be used to get a clear overview on specific subscription, resource groups, resource types or locations.

To search for a specific resource or resources containing a specific name, the **search bar [2]** above the columns can be used. The selected resources based on the **filters [1]** and/or the text in the **search bar [2]** can be **Exported to Excel** with the **Export button [3]** at the right top of the overview.

At the top of the report the **refresh button [4]** is available to refresh the overview.

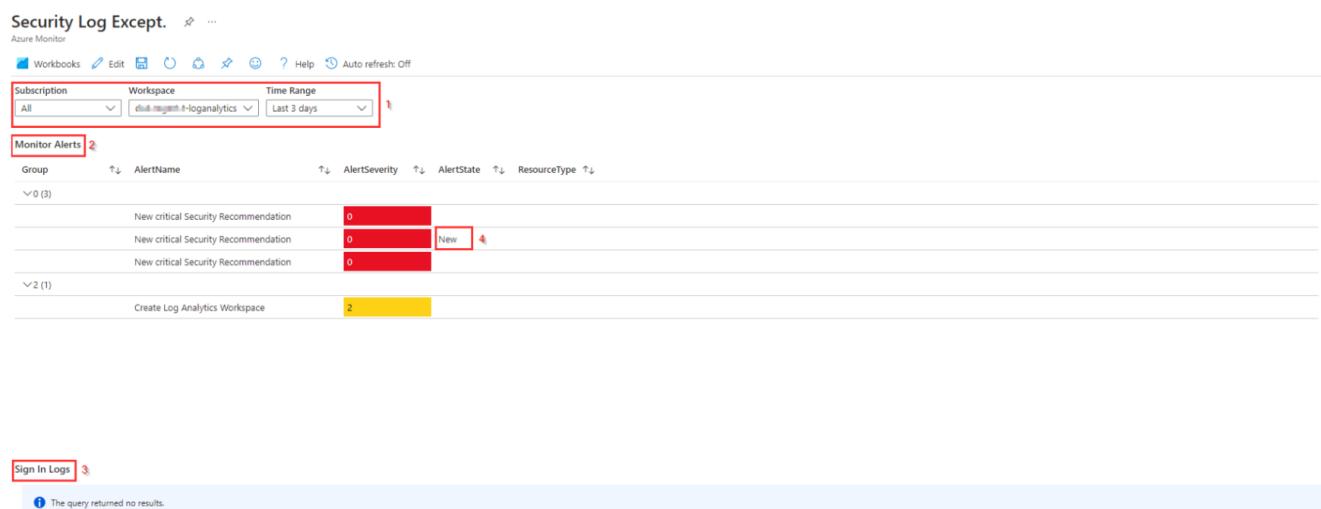
## 9. Security Log Exception workbook

The Security Log Exception Report is a basic report that shows in brief the security log exceptions from the selected log analytics workspace, in 4 separate overviews:

- Monitor Alerts
- Sign In Logs
- Failed Logins
- Security Alerts

On top of this report there are **filters [1]** to select the Subscription (for the log analytics workspace), Workspace and the Time Range.

Based on the selected log analytics workspace(s) and time range the overview for **Monitor Alerts [2]** and **Sign In Logs [3]** will look like this:



The screenshot shows the Azure Monitor interface for a 'Security Log Except.' workbook. At the top, there are filter controls for 'Subscription' (set to 'All'), 'Workspace' (set to 'david-mgmt-loganalytics'), and 'Time Range' (set to 'Last 3 days'). Below these filters is a section titled 'Monitor Alerts' [2]. This section displays a table with columns: Group, AlertName, AlertSeverity, AlertState, and ResourceType. There are three entries under 'New critical Security Recommendation': the first two have '0' in the AlertState column, while the third has 'New' [4] in it. The bottom part of the table shows one entry for 'Create Log Analytics Workspace' with a yellow bar in the AlertState column. Below this table is a section titled 'Sign In Logs' [3]. A message states: 'The query returned no results.'

In the Monitor Alert part, if an Alert is raised in the past 24 hours **New [4]** is added to the AlertState Column.

In the bottom part of this report **Failed Logins [5]** and **Security Alerts [6]** are shown, if any.

Failed Logins 5

ⓘ No Threat Login detected

Security Alerts 0

ⓘ The query returned no results.

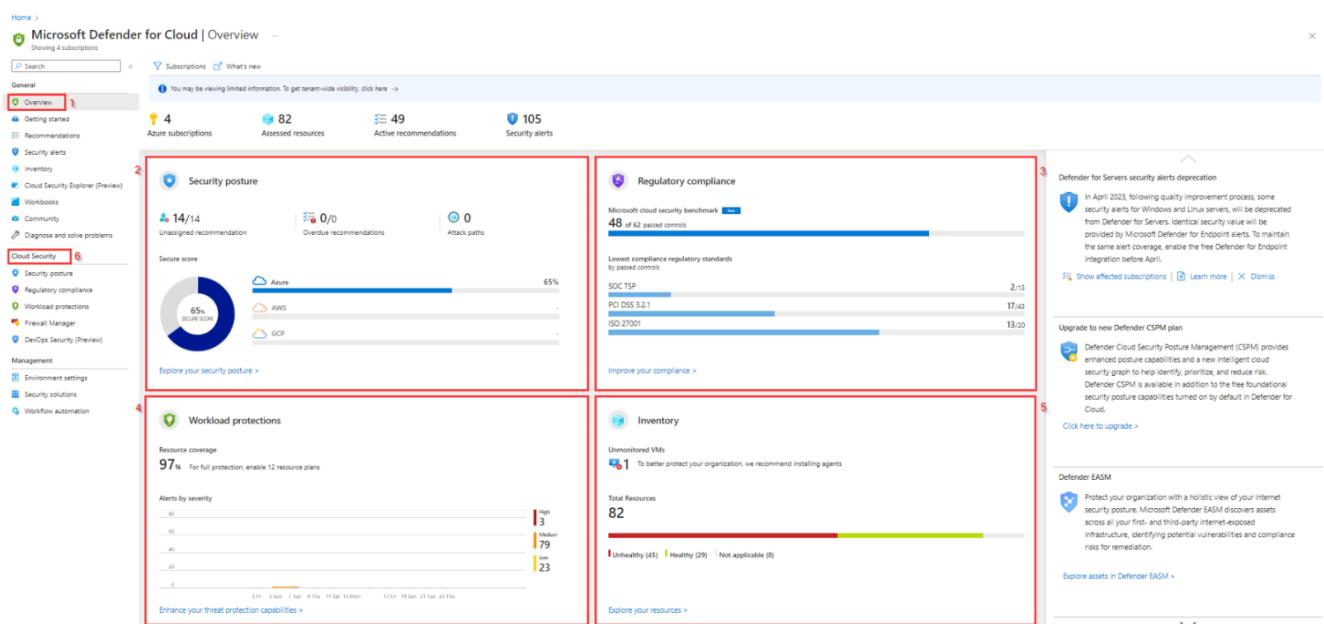
## 10. Compliance report

The Compliancy Report tile redirects you to the Microsoft Defender for Cloud Overview blade in Azure.

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. For more information about Microsoft Defender for Cloud, check this [link](#).

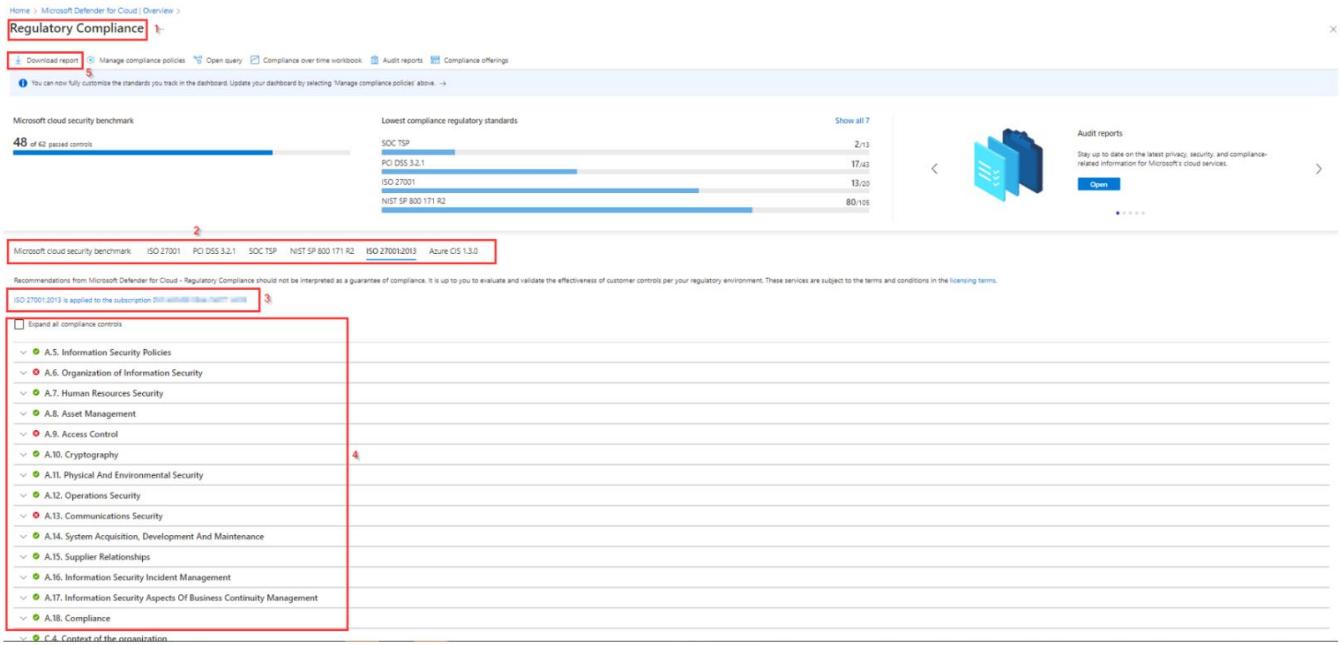
In the **overview blade [1]** of Microsoft Defender for Cloud there are 4 tiles with more detailed Cloud Security information:

- **Security Posture [2]**
- **Regulatory compliance [3]**
- **Workload protections [4]**
- **Inventory [5]**



For Security Posture, Regulatory compliance and Workload protections it is also possible to open this information in a separate blade by selecting the respective blade under **Cloud Security [6]**

By selecting the **Regulatory compliance** tile a separate blade for Regulatory Compliance [1] is opened and shows **compliance standards [2]** that are represented in Defender for Cloud's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.



The screenshot shows the Microsoft Defender for Cloud Regulatory Compliance blade. At the top, there's a navigation bar with links like Home, Microsoft Defender for Cloud Overview, Download report, Manage compliance policies, Open query, Compliance over time workbook, Audit reports, and Compliance offerings. A message says: "You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above." Below this is a chart titled "Lowest compliance regulatory standards" showing progress across various benchmarks:

Benchmark	Progress
ISO 27001	48 of 42 passed controls
PCI DSS 3.2.1	17/43
ISO 27001	13/20
NIST SP 800-171 R2	80/105

On the right, there's an "Audit reports" section with a "View" button. The main area shows a list of compliance controls under "A.5. Information Security Policies", each with a status indicator (green dot for passed, red dot for failing) and a link to details. A red box highlights the "Download report" link [5] at the top of the blade.

For the **selected benchmark [3]** is shown to which subscription the benchmark is applied and an expandable **overview [4]** of the compliance controls is shown.

The compliance report with the results for the selected benchmark can also be downloaded as a PDF or CSV by selecting the **Download report [5]** option on top of this blade.

For more information about the regulatory compliance and the standards that are available in Defender for Cloud check this [link](#)

## 11. Orphan resources workbook

The Orphan Resources report is used to make the orphaned resources per resource type visible. The report has 2 parts:

- The orphaned resource overview blade
- A detailed blade per orphaned resource type

### 11.1 The orphaned resource overview blade

In the top part it is possible to **filter [1]** on Subscription.

When the report is opened by default an **overview [2]** of all possible orphaned resources is displayed together with the number of **orphaned resources [3]** found per type.

Resource Type	Count
Disks	0
Network Interfaces	0
Public IPs	4
Resource Groups	5
Network Security Groups	3
Availability Sets	0
Route Tables	0
Load Balancers	0
App Service Plans	1
Front Door WAF Policy	0
Traffic Manager Profiles	0

Next to the overview blade you will find a more detailed overview with a **separate blade per orphaned resource type [4]** that at this moment is added to this report, like:

- Disks
- Network Interfaces
- Public IPs
- Resource Groups
- Network security groups
- Availability Sets
- Route Tables

- Load Balancers
- App Service Plans
- Front Door WAF Policy
- Traffic Manager Profiles

For more detail about a specific orphaned resource type, you can select the blade for the resource type.

### 11.2 A detailed blade per orphaned resource type

The overview blade only shows the number of orphaned resources per resource type that possibly can contain orphaned resources.

If there are orphaned resources you can select the **blade [1]** for the specific type of resource to show more detailed information about the resource, like in the above picture for the orphaned resource groups:

The screenshot shows the 'Orphan resources' blade in Azure Monitor. At the top, there's a navigation bar with 'Workbooks', 'Edit', 'Azure Monitor', 'Help', and 'Auto refresh: Off'. Below it is a dropdown menu with 'All' selected. The main content area has tabs for 'Resource Groups' (which is highlighted with a red box and labeled 1), 'Network security groups', 'Availability Sets', 'Route Tables', 'Load Balancers', 'App Service Plans', 'Front Door WAF Policy', and 'Traffic Manager Profiles'. The 'Resource Groups' tab displays a summary card with 'Total' (15) and a pie chart showing 'Count by Location' with '5' in the 'westeurope' segment (labeled 2). Below this is a table titled 'Orphan Resource Groups' with columns: Subscription, Search, Location, Tags, and Details. The table lists several entries, each with a 'View Details' button (labeled 3). One entry is highlighted with a red box and labeled 4. A search bar is at the top of the table (labeled 5). A small icon in the top right corner indicates a download or export option (labeled 6).

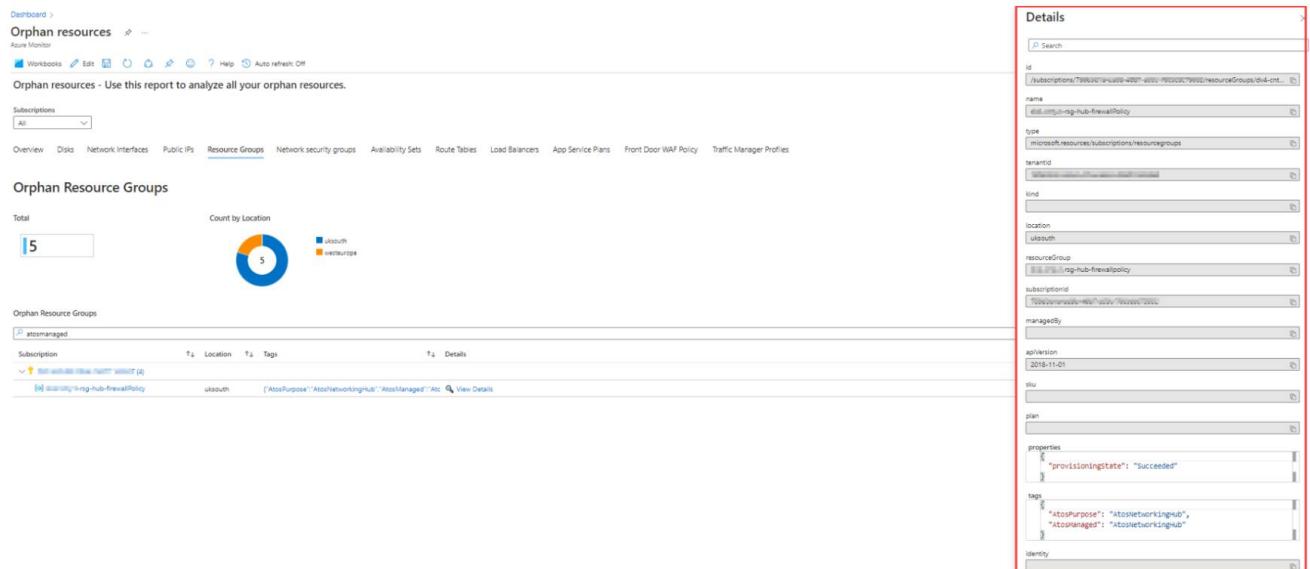
As shown in this blade the **total number of orphaned resource groups together with the count per location [2]** is visible at the top of this blade. In the bottom part you find an overview of the orphaned resource groups **grouped by subscription [3]**.

In this blade it is also possible to select the **name of the resource [4]** to be redirected to the resource it selves, where the orphaned resource can be deleted if needed.

Above the columns is a **searchbar [5]** to search for a specific **resource, location** or resource with a specific **tag**.

At the right side of the resource type blade, you find the **export option [5]** that can be used to download a csv with all resources of this type.

By selecting **View Details [6]** an overview section with more detail about the resource (group) is shown.



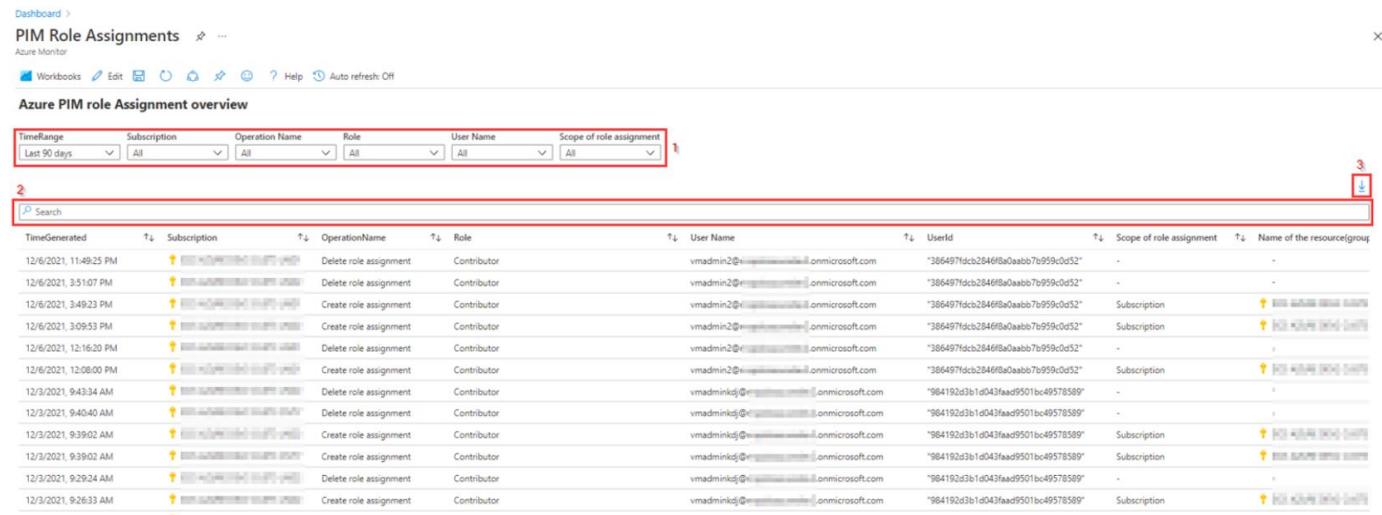
The screenshot shows the Azure portal interface for managing orphan resources. On the left, the 'Orphan resources' blade displays a summary of 5 orphaned resource groups, categorized by location (usouth and westeurope). Below this is a table listing the details of each resource group, including its subscription, location, and tags. One row is selected, highlighting the 'rg-hub-freival' resource group. On the right, a detailed view of this specific resource group is shown in a 'Details' pane. The pane contains various properties of the resource group, such as its ID, name, type, tenant ID, kind, location, resource group, subscription ID, managed by, API version, SKU, plan, properties, tags, and identity.

Subscription	Location	Tags	Details
atomanaged	usouth	[{"AtosPurpose": "AtosNetworkingHub", "AtosManaged": "No"}]	<b>rg-hub-freival</b> usouth [{"AtosPurpose": "AtosNetworkingHub", "AtosManaged": "No"}]

## 12. PIM Role Assignments workbook

The PIM Role Assignments report is used to make the assignments of privileged role for a selected time period visible in an overview.

In the top part the report provides several **filters [1]** to select the **Time Range** and to filter on **Subscription**, **Operation Name** (create or delete), **Role** that is assigned or revoked, **UserName** and **Scope of role assignment** (Subscription, Resource Group, Resource or None (-)).



The screenshot shows the 'Azure PIM role Assignment overview' page. At the top, there are filters for TimeRange (Last 90 days), Subscription (All), Operation Name (All), Role (All), User Name (All), and Scope of role assignment (All). Below the filters is a red-bordered search bar labeled 'Search'. The main area contains a table with columns: TimeGenerated, Subscription, OperationName, Role, User Name, UserId, Scope of role assignment, and Name of the resource/group. The table lists various log entries, such as 'Delete role assignment' for 'Contributor' roles on specific dates like 12/6/2021 and 12/3/2021, and 'Create role assignment' entries. The last row shows a single 'Create role assignment' entry for a 'Contributor' role on 12/3/2021 at 9:26:33 AM.

TimeGenerated	Subscription	OperationName	Role	User Name	UserId	Scope of role assignment	Name of the resource/group
12/6/2021, 11:49:25 PM		Delete role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	-	-
12/6/2021, 3:51:07 PM		Delete role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	-	-
12/6/2021, 3:49:23 PM		Create role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	Subscription	12.3.2021 13:49:23
12/6/2021, 3:09:53 PM		Create role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	Subscription	12.3.2021 15:09:53
12/6/2021, 12:16:20 PM		Delete role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	-	-
12/6/2021, 12:08:00 PM		Create role assignment	Contributor	vmadmin2@*****.onmicrosoft.com	"386497fdc2846fa0aab7b959c0d52"	Subscription	12.3.2021 14:08:00
12/3/2021, 9:43:34 AM		Delete role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	-	-
12/3/2021, 9:40:40 AM		Delete role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	-	-
12/3/2021, 9:39:02 AM		Create role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	Subscription	12.3.2021 10:39:02
12/3/2021, 9:39:02 AM		Create role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	Subscription	12.3.2021 10:39:02
12/3/2021, 9:29:24 AM		Delete role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	-	-
12/3/2021, 9:26:33 AM		Create role assignment	Contributor	vmadminkdj@*****.onmicrosoft.com	"984192d3b1d043faad9501bc49578589"	Subscription	12.3.2021 10:26:33

Underneath the filters there is a **search bar [2]** available for more specific filtering like searching on a specific resource.

The report it selves shows the creation and deletion of role assignments in the following columns:

- TimeGenerated:** time when creation or deletion of role occurred.
- Subscription:** Subscription in which the role is assigned
- OperationName:** Shows the operation, if the role was assigned or deleted from the User account.
- Role:** name of the role that was assigned
- UserName:** Name of the user account that got the role assigned. In most cases this shows the e-mail address of the user if it can be found as this information is only available in the log if the user performed any action in Azure during the selected time range.
- UserId:** Id of the user account that got the role assigned. This information is always available in the log and can be used (if needed) to determine the username.

- **Scope of role assignment:** A role can be assigned to a **Subscription, Resource group** or even to a specific **Resource**. In this column the scope is visible for role assignments. When a role is deleted a dash (-) is visible.
- **Name of the resource(group):** If a role is assigned, this column show to which **Subscription, Resource group** or **Resource** the role is assigned. When a role is deleted a dash (-) is visible.

For the creation of a csv based on the report that is visible, the **download option [5]** at the **right top** above the search bar is available.

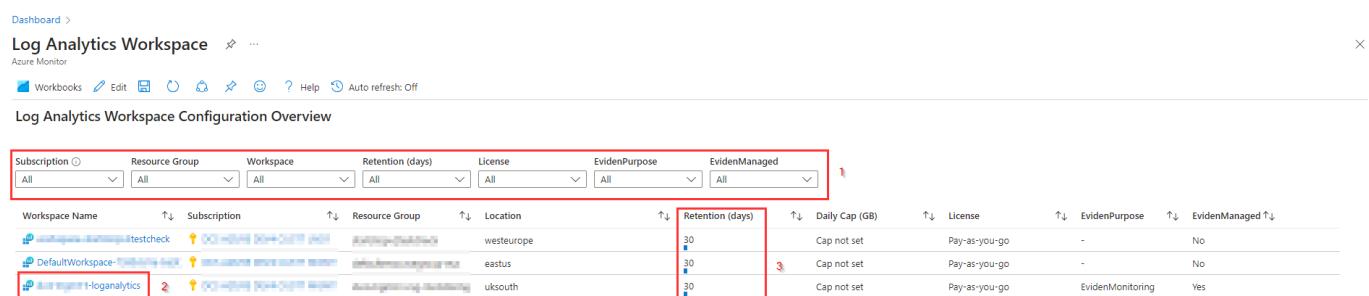
## 13. Log Analytics Workspace workbook

The Log analytics Workspace report consists of 2 parts:

- **Log Analytics Workspace Configuration Overview:** Provides an overview of the Azure Log analytics Workspaces and their configuration that are created in the Azure environment.
- **Log Analytics Workspace Workloads:** An overview of the Log analytics Workspaces with operational data divided in 3 blades:
  - **Health Overview:** Provides an overview of the health of all log analytics workspaces.
  - **Usage Overview:** Graphical overview of the log usage for a selected log analytics workspace and a selected time range.
  - **Detailed Usage:** A detailed overview of the table usage for a selected log analytics workspace and a selected time range.

### 13.1 Log Analytics Workspace Configuration Overview

In the top part it is possible to **filter [1]** on Subscription, Resource Group, Workspace, Retention, Licence, EvidenPurpose tag and if the Log Analytics Workspace is managed by Eviden.



The screenshot shows the 'Log Analytics Workspace Configuration Overview' page. At the top, there are filter dropdowns for Subscription (All), Resource Group (All), Workspace (All), Retention (days) (All), License (All), EvidenPurpose (All), and EvidenManaged (All). Below the filters is a table titled 'Log Analytics Workspace Configuration Overview' with the following columns: Workspace Name, Subscription, Resource Group, Location, Retention (days), Daily Cap (GB), License, EvidenPurpose, and EvidenManaged. The table contains three rows of data. The first row has a 'testcheck' workspace in 'westeurope' with a retention of 30 days, daily cap of 0 GB, pay-as-you-go license, and No EvidenManaged status. The second row has a 'DefaultWorkspace-1' workspace in 'eastus' with a retention of 30 days, daily cap of 0 GB, pay-as-you-go license, and No EvidenManaged status. The third row has a 'LogAnalytics' workspace in 'uksouth' with a retention of 30 days, daily cap of 0 GB, pay-as-you-go license, EvidenMonitoring tag, and Yes EvidenManaged status. A red box highlights the 'Retention (days)' column header and the first three data cells under it.

Workspace Name	Subscription	Resource Group	Location	Retention (days)	Daily Cap (GB)	License	EvidenPurpose	EvidenManaged
testcheck			westeurope	30	Cap not set	Pay-as-you-go	-	No
DefaultWorkspace-1			eastus	30	3 Cap not set	Pay-as-you-go	-	No
LogAnalytics	2		uksouth	30	Cap not set	Pay-as-you-go	EvidenMonitoring	Yes

The report shows an **overview of the Log Analytics Workspaces** that are created with their configuration like **Retention**, **Daily Cap**, **Licence**, **EvidenPurpose** tag and if the **EvidenManaged** tag is set to **Yes**.

For more detail about a Log Analytics Workspace is is possible to select the name of the **Log Analytics Workspace [2]** to open the **Log Analytics Workspace blade**.

In the column **Retention (days) [3]** you will find the retention together with a small graphical view on the number of days for the retention.

## 13.2 Log Analytics Workspace Workloads

The bottom part of the Log Analytics Workspace report provides workload data based on Azure Health and the Azure Logs for Log Analytics Workspace.

The Log Analytics Workspace Workloads reporting part consists of 3 blades:

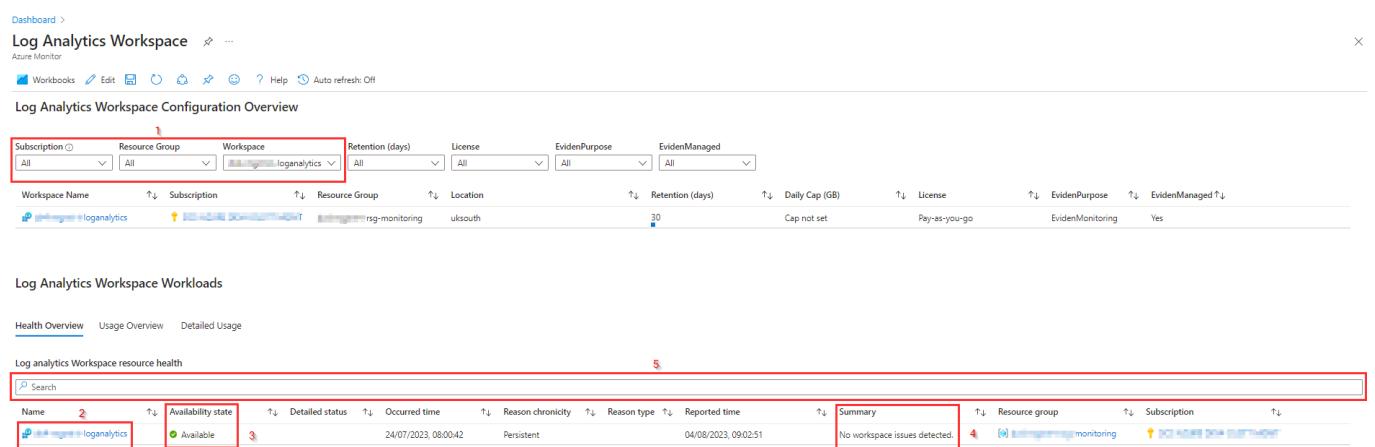
- Health Overview
- Usage Overview
- Detailed Usage

Below the blades are described in more detail

### 13.2.1 Health Overview

For the selected **Subscription(s), Resource Group(s)** and **Workspace(s)** in the **filter [1]** at the top of the report this blade shows an overview with the **health status** of the Log Analytics Workspace(s).

It shows the **Availability State [2]**, **Detailed Status** (if available), the data and time the workspace changed to this state (**Occurred Time**), if the status is Persistent or Transient (**Reason Chronicity**), the **Reason type** and a Summary [3] of the health state. The Summary [3] column adds some more detail in case the log analytics workspace doesn't show Available in the **Availability state [2]** column.



The screenshot shows two blades side-by-side. The left blade is titled 'Log Analytics Workspace Configuration Overview' and displays a table of workspace configurations. The right blade is titled 'Log Analytics Workspace Workloads' and displays a table of workspace health status. Both blades have various filters and sorting options at the top.

Subscription	Resource Group	Workspace	Retention (days)	License	EvidenPurpose	EvidenManaged
All	All	loganalytics	All	All	All	All
Workspace Name	Subscription	Resource Group	Location	Retention (days)	Daily Cap (GB)	License
loganalytics	rg-monitoring	rgs-monitoring	uksouth	30	Cap not set	Pay-as-you-go
					EvidenMonitoring	Yes

Name	2 Availability state	3 Detailed status	Occurred time	Reason chronicity	Reason type	Reported time	5 Search
loganalytics	Available	Persistent	24/07/2023, 08:00:42	04/08/2023, 09:02:51	Summary	No workspace issues detected.	Search bar

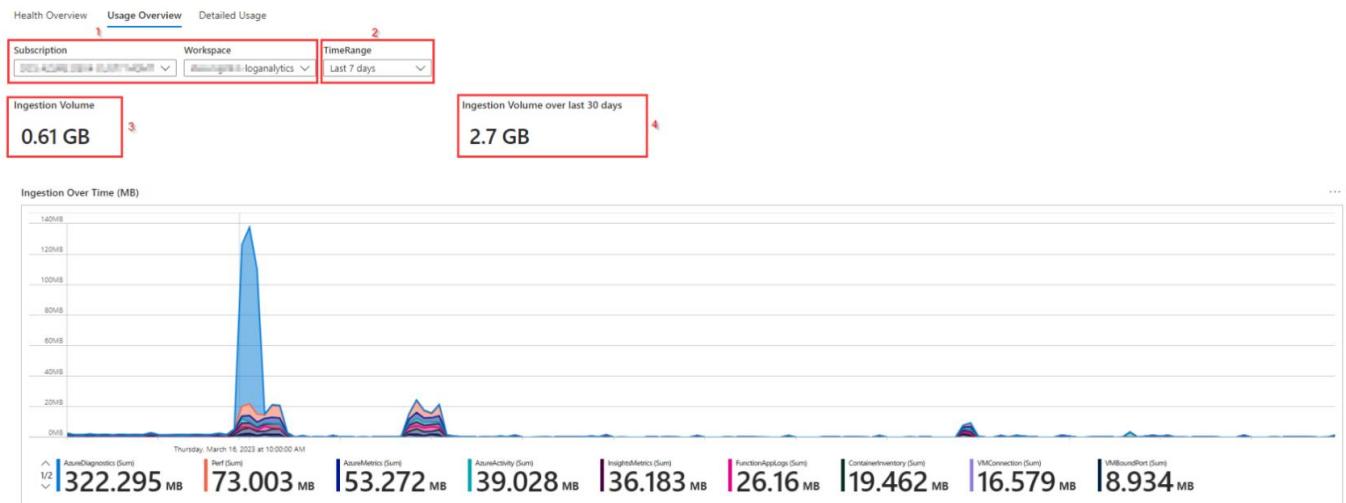
For more detail about a Log Analytics Workspace it is possible to select the **name of the Log Analytics Workspace [4]** to open the **Log Analytics Workspace** blade.

The **searchbar [5]** can be used to search for specific log analytics workspaces.

### 13.2.2 Usage Overview

The Usage Overview provides an overview of the ingestion data volume of a selected Log Analytics Workspace for a selected TimeRange.

The log Analytics workspace can be selected using **the Subscription and the Workspace filter [1]** while the desired time range can be selected using the **TimeRange filter [2]**.



On the top of the overview the total **ingested Volume [3]** is shown, based on the selected Time Range (at the left) and the **ingested volume over the last 30 days [4]**.

At the bottom, a graphical overview is shown with the **Ingestion Over Time** for the logs that are on the selected Log Analytics Workspace.

The screenshot shows the 'Detailed Usage' tab selected. It displays a table of workspace log usage per resource. The columns include Resource Name [4], Resource Id [5], ResourceType, Workspace Log, Billable, and IngestedVolume. A search bar [6] is at the top of the table, and there are export and clear selection buttons [7] on the right. A note at the top of the table states: 'Workspace log usage per resource - be aware that some resources may be deleted already at this moment.'

Resource Name [4]	Resource Id [5]	ResourceType	Workspace Log	Billable	IngestedVolume
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	AzureDiagnostics	Yes	314808275
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	Perf	Yes	53826438
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	ContainerInventory	Yes	19462495
workflows	00000000-0000-0000-0000-000000000000	workflows	AzureDiagnostics	Yes	16237604
sites	00000000-0000-0000-0000-000000000000	sites	FunctionAppLogs	Yes	15599324
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	InsightsMetrics	Yes	14239667
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	FunctionAppLogs	Yes	10958323
redis	00000000-0000-0000-0000-000000000000	redis	AzureMetrics	Yes	8561123
managedclusters	00000000-0000-0000-0000-000000000000	managedclusters	KubePodInventory	Yes	7534604
virtualmachines	00000000-0000-0000-0000-000000000000	virtualmachines	InsightsMetrics	Yes	7387094
sites	00000000-0000-0000-0000-000000000000	sites	AzureMetrics	Yes	7157603

Be ware that the Ingested Volume is based on the selected time range. Based on this it is possible that the resource that is reported is already deleted at the time the report is created. This is also why the name in the **Resource Name [4]** column

is not shown as a link, but instead a separate column has been added with the **Resource Id [5]** that is shown as a link.

In case the resource is already deleted the Resource Id column will sometimes be empty. If the resource is shown as a link, it is still possible that you get an error page when selecting the link.

Use **Billable filter (set to Yes) [3]** to filter out logs that are most used by Azure it selves, like the Azure Activity log or use the **Workspace Log [3]** filter to select a specific log table at the log analytics workspace.

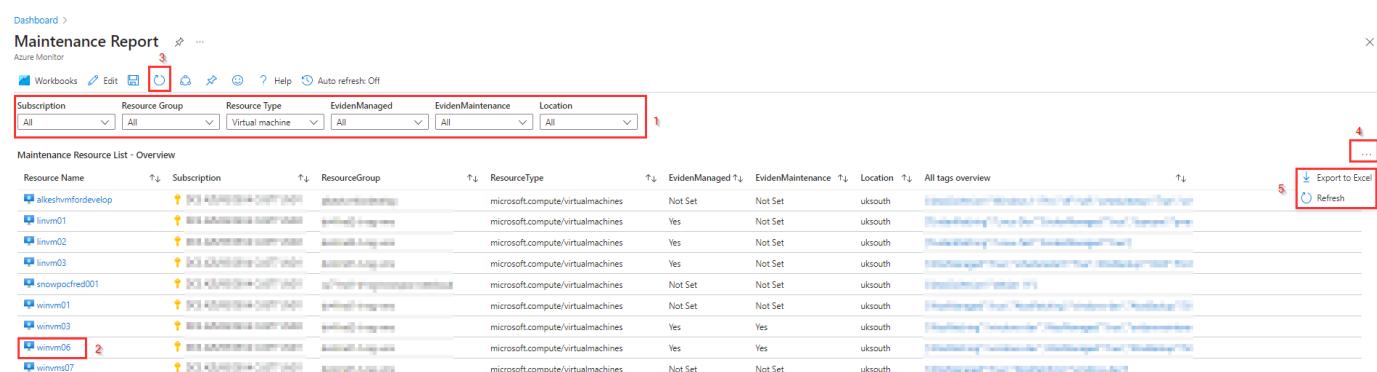
The **searchbar[6]** can be used to search for a specific resource.

You can use the **Export to Excel option [7]** to download the overview to a comma-separated file by first selecting the **three-dots [8]** at the right top of this blade.

## 14. Maintenance workbook

The Maintenance report provides an overview to show if the **EvidenManaged** and **EvidenMaintenance** tags are set to indicate that a resource is Eviden managed and in maintenance. If the resource is in maintenance by setting the **EvidenMaintenance** tag to 'True', no tickets are raised for this resource in case of an alert.

In the top part the report provides several **filters [1]** to select the Subscription, Resource group, Resource type, EvidenManaged tag, EvidenMaintenance tag and Location to report on. This way the filters at the top of the report can be used to get a clear overview of specific resources and EvidenManaged and EvidenMaintenance tag settings.



The screenshot shows the Azure Monitor Maintenance Report interface. At the top, there are several filter dropdowns labeled [1]: Subscription (All), Resource Group (All), Resource Type (Virtual machine), EvidenManaged (All), EvidenMaintenance (All), and Location (All). Below the filters is a table titled "Maintenance Resource List - Overview" [2]. The table has columns: Resource Name, Subscription, ResourceGroup, ResourceType, EvidenManaged, EvidenMaintenance, Location, and All tags overview. The table lists several virtual machines: alikeshvmfordevelop, linvm01, linvm02, linvm03, snowpackred001, winvm01, winvm03, winvm06 (highlighted with a red box and a red question mark [2]), and winvm07. The "winvm06" row shows EvidenManaged as Yes and EvidenMaintenance as Yes. On the right side of the interface, there are three dots [4] which lead to "Export to Excel" and "Refresh" options [5].

To change the value of a tag or define a tag, you can click on the **Resource Name [2]** in the report as this opens the blade for the selected Resource and make the changed in the **Overview blade**. It will take 10-15 seconds before the new value for a tag is visible in the report. You need to click on **refresh [3]** to get the new value displayed in the report.

When you select the **three-dots [4]** in the right top you find the **Export to Excel and the refresh option [5]**

## 15. Virtual WAN workbook

The Virtual WAN report is used to provide an overview of the Virtual WAN(s) deployed in the Azure environment together with all Virtual WAN related resources.

The report consists of several blades, starting with an overview followed with more detail for each resource that is part of the virtual WAN solution:

- **Overview blade:** Overview of deployed Virtual WAN solutions with configuration information, configured hubs and hub virtual network connection.
- **VPN Gateways blade:** Overview of VPN Gateways with hub connected to and configuration.
- **VPN Sites blade:** Overview of Virtual WAN VPN Sites with configuration, VPN Site links and status of the VPN Site links.
- **ExpressRoute Gateways blade:** Overview of ExpressRoute Gateways with configuration and ExpressRoute connections.

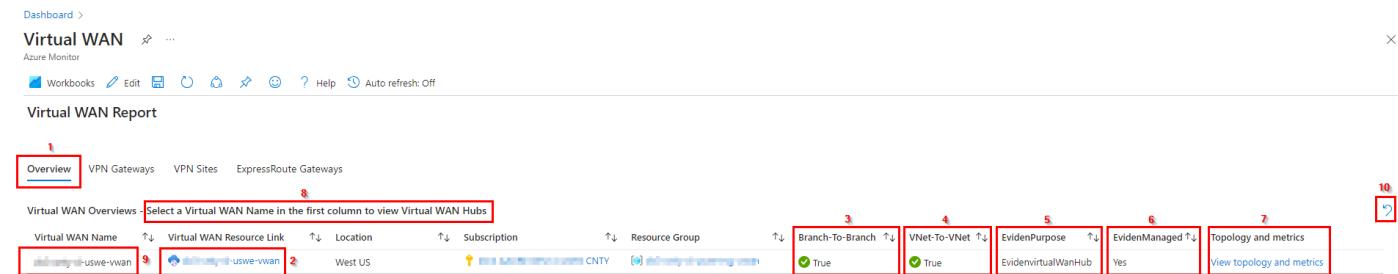
Below each blade is described in more detail

### 15.1 Overview blade

The **Overview** blade consists of three parts:

- Virtual WAN Overviews
- Virtual WAN Hubs
- Virtual WAN – Hubs – Connections/Peering

The **Virtual WAN Overviews** [1] part in the Overview blade as visible below shows an overview of the deployed Virtual WAN solutions.



The screenshot shows the 'Virtual WAN Report' blade in the Azure portal. At the top, there are tabs for 'Overview', 'VPN Gateways', 'VPN Sites', and 'ExpressRoute Gateways'. The 'Overview' tab is selected. Below the tabs, there is a search bar with the placeholder 'Select a Virtual WAN Name in the first column to view Virtual WAN Hubs'. The main area contains a table with the following columns and data:

Virtual WAN Name	Virtual WAN Resource Link	Location	Subscription	Resource Group	Branch-To-Branch	VNet-To-VNet	EvidenPurpose	EvidenManaged	Topology and metrics
<a href="#">uswe-wan</a>	<a href="#">uswe-wan</a>	West US	CNTY	cnty-vnet	True	True	EvidenVirtualWanHub	Yes	<a href="#">View topology and metrics</a>

The **Virtual WAN Resource Link** [2] column contains the Virtual WAN name as a link that will redirect to the Virtual WAN resource in Azure. The columns **Branch-To-Branch** [3] and **VNet-To-VNet** [4] show if branch to branch and vnet to vnet traffic is allowed for the virtual WAN.

The **EvidenPurpose [5]** shows the value for the EvidenPurpose tag, while the **EvidenManaged [6]** column shows if the Virtual WAN is managed by Eviden or not.

In the last column, **Topology and metrics [7]**, a link is available to *View topology and metrics*. This link redirects to an overview that shows but the topology and the metrics blade for the selected Virtual WAN in the (default) Azure environment.

The screenshot shows the Azure portal interface for a Virtual WAN named 'dell-unity-d-usw1-vwan'. On the left, there's a search bar and a 'Download topology' button. The main area displays a network topology diagram with a central hub and several spoke regions. In the top right, there's a 'Metrics' blade titled 'Network Insights VirtualWANs Minified' showing 'Virtual WAN: dell-unity-d-usw1-vwan' and a time range of 'Last 24 hours'. Below it, the 'Virtual WAN Hub Capacities' table shows one Virtual Hub with 1 VPN Gateway Scale Unit, 1 P2S Gateway Scale Unit, and 1 ER Gateway Scale Unit. The 'S2S Gateway Average Bandwidth' chart shows a line graph with a value of 7.99 b/s.

**Remark:** this blade can only be shown using this link if the Virtual WAN is same customer environment as is configured as the default (Startup) environment in Azure.

If the topology blade fails to load, first select the **Virtual WAN resource link [2]** in the overview and in the Virtual WAN resource link select **View Topology** as shown below to open this blade in Azure.

The screenshot shows the Azure portal interface for the 'Virtual WAN' resource link of the 'dell-unity-d-usw1-vwan' Virtual WAN. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Settings', and 'Configuration'. The main panel shows the 'Essentials' section with details like Resource group, Location (West US), Subscription, and Subscription ID. It also shows Tags (edit) with 'EvidenManaged : true' and 'EvidenPurpose : EvidenvirtualWanHub'. The 'Topology' section includes a status of 'Succeeded', Branch-to-branch status, Virtual hubs count (1), and a 'View Topology' link which is highlighted with a red box.

In the overview part of this blade there is the option to **Select a Virtual WAN Name in de first column to view Virtual WAN Hubs [8]**.

This means that you can select the name of the virtual WAN in the **Virtual WAN Name [9]** column and then the configured Virtual WAN Hubs for that virtual WAN are visible in the middle part of the **Overview [1]** blade, like in this picture:

Dashboard > Virtual WAN ...

Azure Monitor

Workbooks Edit Help Auto refresh: Off

Virtual WAN Report

**1** Overview VPN Gateways VPN Sites ExpressRoute Gateways

Virtual WAN Overviews - Select a Virtual WAN Name in the first column to view Virtual WAN Hubs

Virtual WAN Name	Virtual WAN Resource Link	Location	Subscription	Resource Group	Branch-To-Branch	VNet-To-VNet	EvidenPurpose	EvidenManaged	Topology and metrics
HubName@uswe-vwan	HubName@uswe-vwan	West US	CNTY	child virtualwanresource	True	True	Evidenvirtualwanhub	Yes	<a href="#">View topology and metrics</a>

Hub Name	Hub Resource Link	Virtual WAN	Location	Subscription	Resource Group	Secured Hub	AddressPrefix	SKU	Branch-To-Branch
HubName@uswe-vwan-hub	HubName@uswe-vwan-hub	HubName@uswe-vwan	West US	CNTY	child virtualwanresource	child virtualfw-hub	10.200.0.0/23	Standard	False

**8** Select a Hub Name in the first column to view Hub VirtualNetwork Connections

**10** 

Using the **counter wise pointing arrow [10]** the selection can be cleared, and the middle part of this blade will disappear again.

The **Hub Resource Link [2]** column contains the Virtual WAN Hub name as a link that will redirect to the Virtual WAN Hub resource in Azure. The column **Virtual WAN [3]** contains the name of the virtual WAN the hub is connected to and is provided as a link to the virtual WAN resource.

When the hub is secured by a firewall, the link to the firewall resource is provided in the **Secured Hub [4]** column.

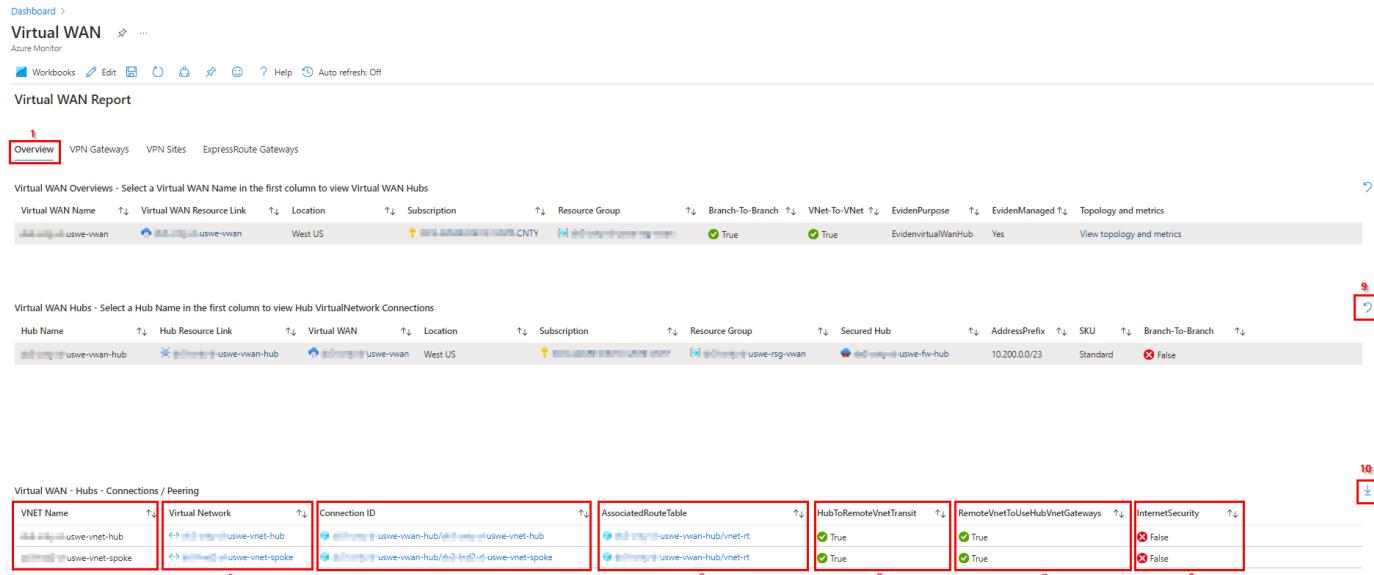
The **AddressPrefix [5]** column shows the private address space that is configured for the virtual hub.

In the **SKU [6]** column the hub type is shown. This can be **Basic** (for Site-to-site VPN configurations only) or **Standard** (support ExpressRoute, point-to-site (User VPN), a full mesh hub, and VNet-to-VNet transit through the Azure hubs).

**Branch-To-Branch [8]** show if branch to branch is allowed for the virtual hub.

In the middle part of this blade there is the option to **Select a Hub Name in the first column to view Hub VirtualNetwork Connections [8]**.

This means that you can select the name of the virtual hub in the **Hub Name [9]** column and then the configured hub virtual network connections for that virtual hub are visible in the bottom part of the **Overview [1]** blade, like in this picture:



The screenshot shows the Azure Virtual WAN Overview blade. At the top, there are tabs for Overview, VPN Gateways, VPN Sites, and ExpressRoute Gateways. The Overview tab is selected. Below the tabs, there are two main sections:

- Virtual WAN Overviews:** A table with columns: Virtual WAN Name, Virtual WAN Resource Link, Location, Subscription, Resource Group, Branch-To-Branch, VNet-To-VNet, EvidenPurpose, EvidenManaged, and Topology and metrics. One row is shown: uswe-vwan, uswe-vwan, West US, CNTY, True, True, EvidenvirtualWanHub, Yes, and a link to View topology and metrics.
- Virtual WAN Hubs:** A table with columns: Hub Name, Hub Resource Link, Virtual WAN, Location, Subscription, Resource Group, Secured Hub, AddressPrefix, SKU, Branch-To-Branch. One row is shown: uswe-vwan-hub, uswe-vwan-hub, uswe-vwan, West US, uswe-vwan-hub, uswe-rsg-vwan, 10.200.0.0/23, Standard, False.

At the bottom, there is a section titled "Virtual WAN - Hubs - Connections / Peering" with columns: VNET Name, Virtual Network, Connection ID, AssociatedRouteTable, HubToRemoteVNetTransit, RemoteVnetToUseHubVnetGateways, and InternetSecurity. Two rows are shown:

VNET Name	Virtual Network	Connection ID	AssociatedRouteTable	HubToRemoteVNetTransit	RemoteVnetToUseHubVnetGateways	InternetSecurity
uswe-vnet-hub	uswe-vnet-hub uswe-vnet-spoke	uswe-vnet-hub uswe-vnet-spoke	uswe-vwan-hub/vnet-rt uswe-vwan-hub/vnet-rt	True True	True True	False False

Annotations with numbers 1 through 10 point to specific UI elements: 1 points to the Overview tab; 2 points to the VNET Name column; 3 points to the Virtual Network column; 4 points to the Connection ID column; 5 points to the AssociatedRouteTable column; 6 points to the HubToRemoteVNetTransit column; 7 points to the RemoteVnetToUseHubVnetGateways column; 8 points to the InternetSecurity column; 9 points to a counter-wise pointing arrow; 10 points to a down-pointing arrow.

With this bottom part the overview blade is complete. In the first column of this part the **VNet Name [2]** is shown followed by a **Virtual Network [3]** column that contains the link to the VNet. By clicking this link, you will be redirected to the virtual network blade in Azure.

The **Connection ID [4]** column shows the link to the hub virtual network connection, while the **AssociatedRouteTable [5]** column shows the link to the hub route table that is associated to the connection.

When the **HubToRemoteVNetTransit [6]** column shows **True**, virtual hub to remote vnet transit is enabled. **RemoteVnetToUseHubVnetGateways [7]** column shows if remote vnet to use virtual hub's gateways is allowed (**True**) or not (**False**).

The **InternetSecurity [8]** column shows if internet security is enabled (**True**) for this connection or not (**False**).

Using the **counter wise pointing arrow [9]** the selection can be cleared, and the bottom part of this blade will disappear again.

When selecting the **down pointing arrow [10]**, the Virtual WAN – Hubs – Connections/Peering will be exported as a csv.

## 15.2 VPN Gateways blade

The **VPN Gateways [1]** blade as shown in the picture below, gives an overview of the VPN Gateways that are deployed in the environment.

Dashboard >  
Virtual WAN < ...  
Azure Monitor

Workbooks Edit ⌂ ⌂ ? Help Auto refresh: Off

Virtual WAN Report

Overview	VPN Gateways	VPN Sites	ExpressRoute Gateways
Virtual WAN - VPN Gateways	<b>2</b> VPN Gateway  uswe-vpn-wan	<b>3</b> Hub  uswe-vwan-hub	Location ↑ Resource Group ↑ Subscription ↑ <b>4</b> EvidenPurpose ↑ EvidenvirtualWanHub
			<b>5</b> EvidenManaged ↑ Yes
			<b>6</b> VPN Gateway Scale Unit ↑ 1
			<b>7</b> BGP Route Translation For Nat ↑ false
			<b>8</b> Routing Preference Internet false

The **VPN Gateway [2]** column shows the name of the VPN gateway provided as a link that redirects you to the resource blade for the VPN Gateway.

In the **Hub [3]** column the virtual hub, where the VPN Gateway is connected to is shown. This is also a link to the virtual hub resource blade in Azure.

The **EvidenPurpose [4]** shows the value for the EvidenPurpose tag, while the **EvidenManaged [5]** column shows if the Virtual WAN is managed by Eviden or not.

The **VPN Gateway Scale Unit [6]** column shows the number of scale units configured for the VPN Gateway. A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps. Example: 10 scale unit of VPN would imply  $500 \text{ Mbps} * 10 = 5 \text{ Gbps}$ .

The **Enable BGP Route Translation For NAT [7]** shows if this setting is enabled (**True**) or not (**False**). For more information on this setting check this [link](#).

The **Routing Preference Internet [8]** column shows if the routing preference is set to internet (**True**) or not (**False**). For more information on the routing preference setting check this [link](#).

## 15.3 VPN Sites blade

The **VPN Sites [1]** blade provides an overview of the configured virtual wan vpn sites. For this this blade contains two parts:

- Virtual WAN VPN Sites
- Virtual WAN – VPN – Sites Links

When this blade is opened, only the top part appears as visible in the picture on the next page. This Virtual WAN VPN Sites overview will be described first.

In the **VPN Site Name [2]** column of this overview the name of the VPN Site is shown. In the **VPN Site Resource Link [3]** column the name of the VPN Site is shown as a link that will redirect to the VPN site blade in Azure.

Dashboard > Virtual WAN > ...

Azure Monitor

Workbooks Edit ⌂ ⌂ ⌂ ⌂ ⌂ Help Auto refresh: Off

Virtual WAN Report

Overview VPN Gateways **VPN Sites** ExpressRoute Gateways

Virtual WAN VPN Sites - Select a VPN Site Name in the first column to view VPN site links [11]

Virtual Site Name	VPN Site Resource link	Virtual WAN	Hub	VPN Gateway	Location	Resource Group	Subscription	AddressPrefixes	DeviceVendor	VPNSiteLinks
Site1	Site1	uswe-vwan	uswe-vwan-hub	uswe-vpn-vwan	West US	[{"name": "uswe-rsg-vwan"}]	[{"name": "cnty"}]	[{"prefix": "10.0.0.0/24"}]	Microsoft	[{"properties": {"provisioningState": "Succeeded", "ipAddress": "40.83.143.128", "linkProperties": {"linkSpeedInMbps": 50, "linkProviderName": "Microsoft"}, "bgpProperties": {"bgpPeeringAddress": "192.168.0.228", "bgpLocalAddress": "192.168.0.228", "bgpLocalASN": 64456}}]
Site2	Site2	uswe-vwan	uswe-vwan-hub	uswe-vpn-vwan	West US	[{"name": "uswe-rsg-vwan"}]	[{"name": "cnty"}]	[{"prefix": "10.0.0.0/24"}]	Microsoft	[{"properties": {"provisioningState": "Succeeded", "ipAddress": "40.83.143.128", "linkProperties": {"linkSpeedInMbps": 50, "linkProviderName": "Microsoft"}, "bgpProperties": {"bgpPeeringAddress": "192.168.0.228", "bgpLocalAddress": "192.168.0.228", "bgpLocalASN": 64456}}]

12

The columns **Virtual WAN [4]**, **Hub [5]** and **VPN Gateway [6]** show the links to the respective Virtual WAN, Hub and VPN Gateway the Site is connected to.

The **AddressPrefixes [7]** column show the configured address blocks, if any configured and the **DeviceVendor [8]** the name of the device vendor for the site-to-site connection. For more information on this and a list of device vendors check this [link](#).

The **VPNSiteLinks [9]** column contains the properties of the site links in json format. When the properties are opened a detailed overview like this is opened:

Details

Search

```
0
{
  "properties": {
    "provisioningState": "Succeeded",
    "ipAddress": "40.83.143.128",
    "linkProperties": {
      "linkSpeedInMbps": 50,
      "linkProviderName": "Microsoft"
    },
    "bgpProperties": {
      "bgpPeeringAddress": "192.168.0.228",
      "bgpLocalAddress": "192.168.0.228",
      "bgpLocalASN": 64456
    }
  }
}
```

When you **Select a VPN Site Name in the first column to view VPN site links [11]** a separate overview will show up at the bottom part of this blade with the VPN Site links. Using the **counter wise pointing arrow [12]** the selection can be cleared, and the bottom part of this blade will disappear again.

The VPN Sites blade with the **Virtual WAN - VPN - Sites Links [1]** part will look like this:

Dashboard > Virtual WAN > ...

Azure Monitor

Workbooks Edit ⌂ ⌂ ⌂ ⌂ ⌂ Help Auto refresh: Off

Virtual WAN Report

Overview VPN Gateways **VPN Sites** ExpressRoute Gateways

Virtual WAN VPN Sites - Select a VPN Site Name in the first column to view VPN site links

Virtual Site Name	VPN Site Resource link	Virtual WAN	Hub	VPN Gateway	Location	Resource Group	Subscription	AddressPrefixes	DeviceVendor	VPNSiteLinks
Site1	Site1	uswe-vwan	uswe-vwan-hub	uswe-vpn-vwan	West US	[{"name": "uswe-rsg-vwan"}]	[{"name": "cnty"}]	[{"prefix": "10.0.0.0/24"}]	Microsoft	[{"properties": {"provisioningState": "Succeeded", "ipAddress": "40.83.143.128", "linkProperties": {"linkSpeedInMbps": 50, "linkProviderName": "Microsoft"}, "bgpProperties": {"bgpPeeringAddress": "192.168.0.228", "bgpLocalAddress": "192.168.0.228", "bgpLocalASN": 64456}}]
Site2	Site2	uswe-vwan	uswe-vwan-hub	uswe-vpn-vwan	West US	[{"name": "uswe-rsg-vwan"}]	[{"name": "cnty"}]	[{"prefix": "10.0.0.0/24"}]	Microsoft	[{"properties": {"provisioningState": "Succeeded", "ipAddress": "40.83.143.128", "linkProperties": {"linkSpeedInMbps": 50, "linkProviderName": "Microsoft"}, "bgpProperties": {"bgpPeeringAddress": "192.168.0.228", "bgpLocalAddress": "192.168.0.228", "bgpLocalASN": 64456}}]

**Virtual WAN - VPN - Sites Links**

VPN Site Link Name	Connectivity Status	Last Status Change	Link Provider Name	Speed In Mbps	Link IP Address/FQDN	Link BGP Address	Link ASN
Site1/Link1	Connected	10/23/2023, 4:04:37 PM	Microsoft	50	40.83.143.128	192.168.0.228	64456

The first column shows the **VPN Site Link Name [2]**. This is a link that will redirect to the site/link blade in Azure.

The **Connectivity Status [3]** column shows the connectivity status of the link. As the connectivity status need to be checked separately it sometimes takes some time before the bottom part appears after the VPN Site Name is selected in the top part of this overview. In the **Last Status Change [4]** column, when this Connectivity Status was reached.

The **Link Provider Name [5]** shows the name of the vendor that provides the link and is in most cases the same as the DeviceVendor as shown in the top part of this blade.

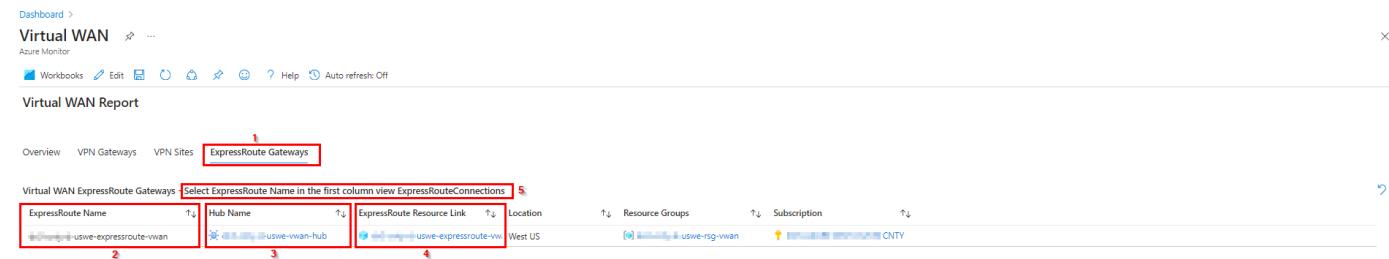
The next columns show the configuration information for the link like **Speed in Mbps [6]**, **Link IP Address/FQDN [7]**, **Link BGP Address [8]** and **Link ASN [9]**.

## 15.4 ExpressRoute Gateways blade

The **ExpressRoute Gateways [1]** blade provides an overview of the configured ExpressRoute Gateways. For this this blade contains two parts:

- Virtual WAN ExpressRoute Gateways
- Virtual WAN - ExpressRoute Connection List

When this blade is opened, only the top part appears as visible in the picture on the next page. This Virtual WAN ExpressRoute Gateways overview will be described first.



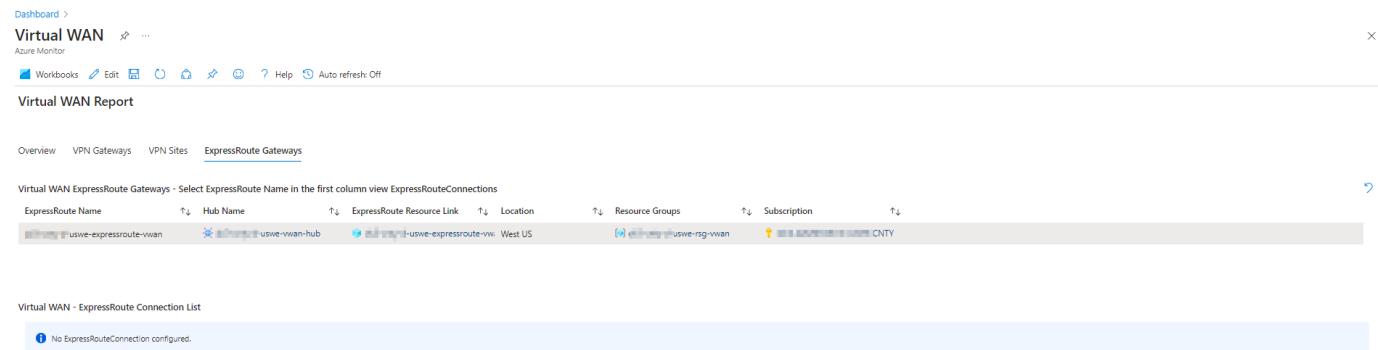
Virtual WAN ExpressRoute Gateways				
Select ExpressRoute Name in the first column view ExpressRouteConnections 5				
ExpressRoute Name	Hub Name	ExpressRoute Resource Link	Location	
uswe-expressroute-vwan	uswe-usvwan-hub	uswe-expressroute-vwan	West US	<a href="#">Resource Groups</a> <a href="#">Subscription</a> <a href="#">CNTV</a>

The **ExpressRoute Name [2]** shows the name of the ExpressRoute gateway, while in the **ExpressRoute Resource Link [4]** column the link to the ExpressRoute Azure blade can be found.

In the **Hub Name [3]** column the link to the Virtual Hub where the ExpressRoute Gateway is connected to is shown.

In this overview you can **Select ExpressRoute Name in the first column view ExpressRouteConnections [5]** to get an overview of the ExpressRoute

connections for the selected ExpressRoute gateway in the bottom part of this overview.



In this example there are no ExpressRoute Connections available due to the costs of these connections, but in case they are configured the following columns will be visible in for the connections:

- **ExpressRoute Connection:** a link to the ExpressRoute Connection blade in Azure.
- **ExpressRouteCircuitPeering:** This can be Private or Microsoft peering. Check this [link](#) for more information on this.
- **RoutingWeight:** shows the connection weight of this ExpressRoute connection. For more information check this [link](#).
- **Enable Internet Security:** Enable internet security. The value can be **True** or **False**.
- **ExpressRouteGatewayBypass:** Enable FastPath to vWan Firewall hub. The value can be **True** or **False**.
- **RoutingConfiguration:** The Routing Configuration indicating the associated and propagated route tables on this connection.