

## Integrating Microsoft Azure

<https://campus.barracuda.com/doc/100370063/>

Barracuda XDR retrieves Audit Logs, Sign In Logs, and Activity Logs from Microsoft Azure. These items are read from the Azure Event Hub.

**Barracuda**Campus



# BarracudaCampus



Videolink:

<https://campus.barracuda.com/>

This video has no sound.

## Requirements

- An Azure Premium **P1 or P2** license is required.

Integrating Microsoft Azure requires you follow these procedures, below:

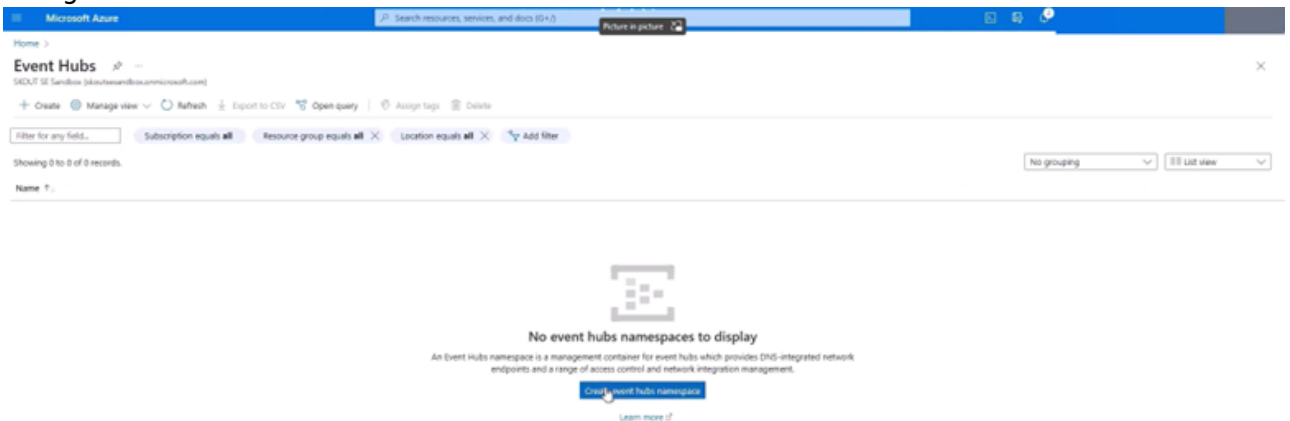
- **Part 1: Setting Up Azure Event Hub**
  - To create Event Hub Namespaces
- **Part 2: Configuring Storage Accounts**
  - To initialize Storage Accounts
  - To set up Event Hub Entities
  - To set up an Event Hub Shared Access Policy
- **Part 3: Updating Diagnostic Settings**

- To update diagnostic settings for the sign in log
  - To update diagnostic settings for the audit log and activity log
  - To set up Microsoft Defender for Cloud
- **Part 4: Barracuda XDR Dashboard Setup for Azure**

## Part 1: Setting Up Azure Event Hub

### To create Event Hub Namespaces

1. Navigate to the Azure Event Hub.



2. Create three event hub namespaces dedicated to each of the following:
  1. Audit Logs
  2. Sign In Logs
  3. Activity Logs

The **Event Hub Namespace Name** must:

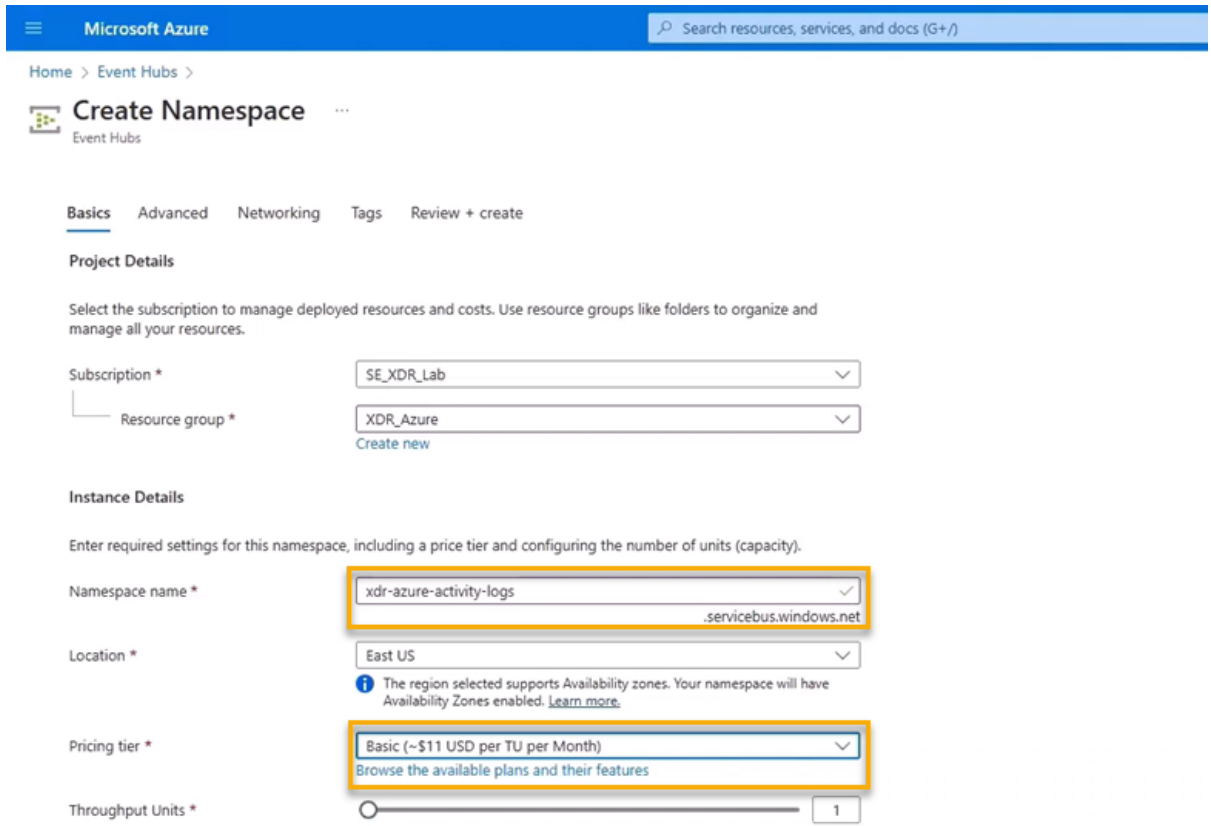
- Contain at least eight characters.
- Not contain special characters.

In **Pricing Tier**, select **Basic**.

In **Networking**, select **Public Access**.

We recommend the following naming convention:

- xdr-azure-activity-logs
- xdr-azure-audit-logs
- xdr-azure-sign-in-logs



Microsoft Azure

Home > Event Hubs >

## Create Namespace

Event Hubs

Basics Advanced Networking Tags Review + create

### Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* SE\_XDR\_Lab

Resource group \* XDR\_Azure  
[Create new](#)

### Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name \* xdr-azure-activity-logs  
.servicebus.windows.net

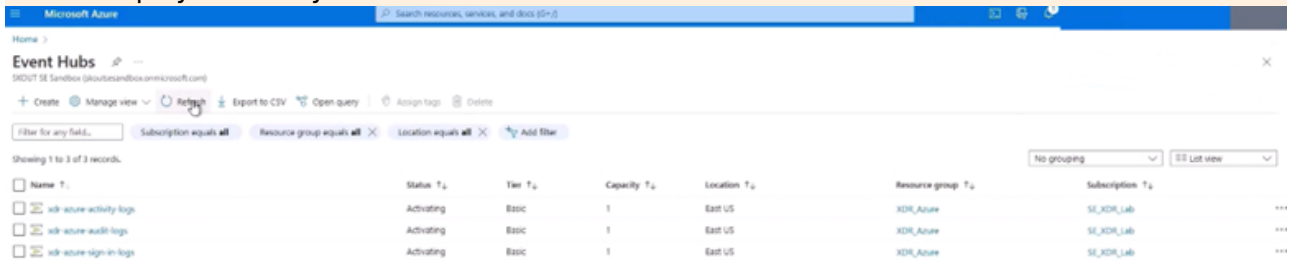
Location \* East US  
The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more](#).

Pricing tier \* Basic (~\$11 USD per TU per Month)  
[Browse the available plans and their features](#)

Throughput Units \* 1

### 3. Click **Review and Create**.

The deployment may take a while.



Name	Status	Tier	Capacity	Location	Resource group	Subscription
xdr-azure-activity-logs	Activating	Basic	1	East US	XDR_Azure	SE_XDR_Lab
xdr-azure-audit-logs	Activating	Basic	1	East US	XDR_Azure	SE_XDR_Lab
xdr-azure-sign-in-logs	Activating	Basic	1	East US	XDR_Azure	SE_XDR_Lab

## Part 2: Configuring Storage Accounts

Configuring storage accounts requires the following procedures, below:

- To initialize Storage Accounts
- To set up Event Hub Entities
- To set up an Event Hub Shared Access Policy

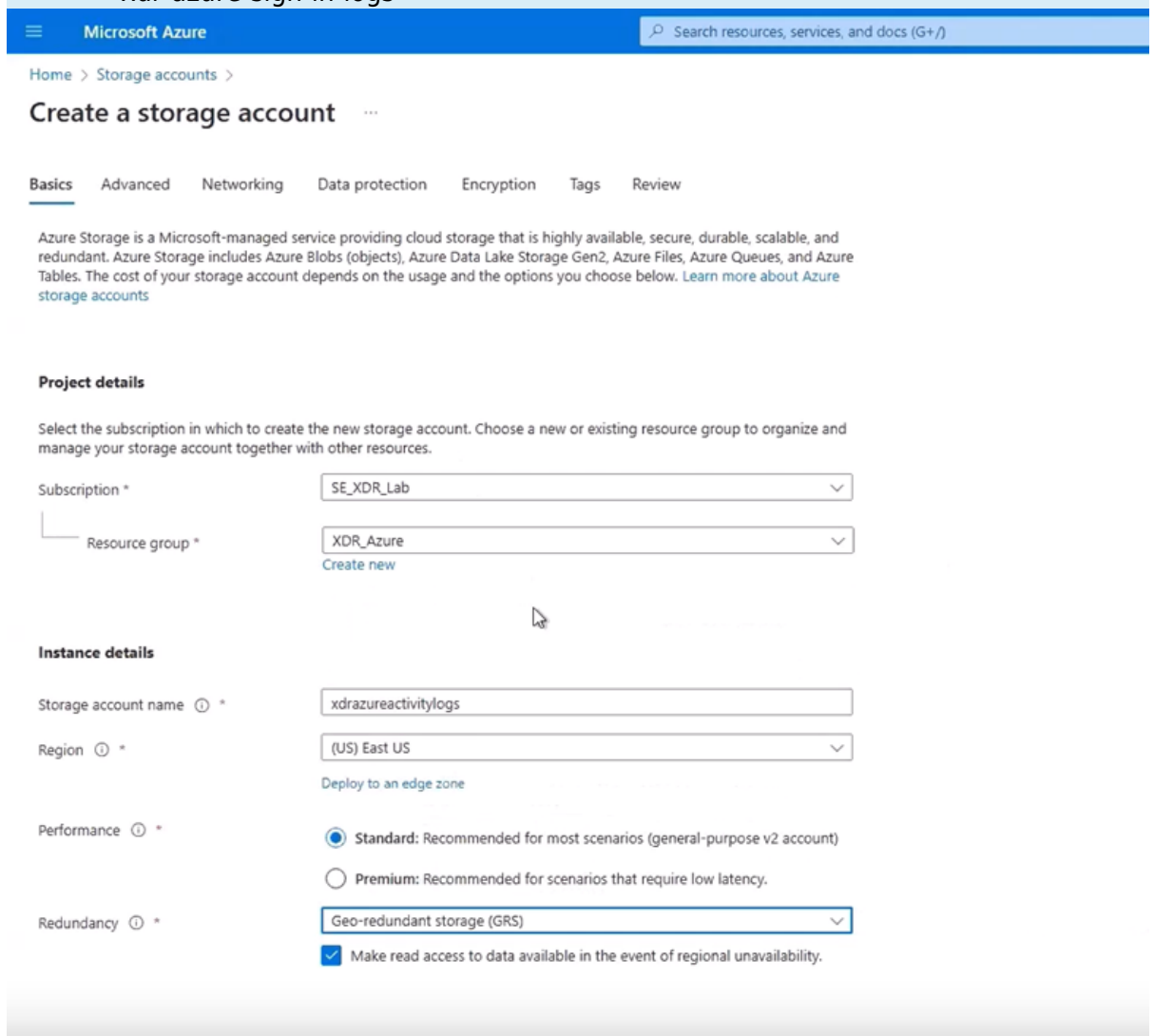
## To initialize storage accounts

### 1. Navigate to **Storage Accounts**.

- Audit Logs
- Sign In Logs
- Activity Logs

We recommend the following naming convention:

- xdr-azure-activity-logs
- xdr-azure-audit-logs
- xdr-azure-sign-in-logs



Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Storage accounts >

## Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \* SE\_XDR\_Lab

Resource group \* XDR\_Azure  
[Create new](#)

### Instance details

Storage account name ⓘ \* xdrazureactivitylogs

Region ⓘ \* (US) East US  
[Deploy to an edge zone](#)

Performance ⓘ \*

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)

☐ **Premium:** Recommended for scenarios that require low latency.

Redundancy ⓘ \*

Geo-redundant storage (GRS)

☒ Make read access to data available in the event of regional unavailability.

### 2. Click **Review and Create**.

The deployment may take a while.

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

## Storage accounts

SKOUT SE Sandbox (skoutsesandbox.onmicrosoft.com)

+ Create Restore Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 3 of 3 records.

Name	Type	Kind	Resource group
xdrazureactivitylogs	Storage account	StorageV2	XDR_Azure
xdrazureauditlogs	Storage account	StorageV2	XDR_Azure
xdrazureloginlogs	Storage account	StorageV2	XDR_Azure

## To set up Event Hub Entities

1. In Microsoft Azure, navigate to **Event Hubs**.
2. In **Event Hubs**, select the check box of an **Event Hub Namespace** that you created in the previous procedure.

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

## Event Hubs

SKOUT SE Sandbox (skoutsesandbox.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

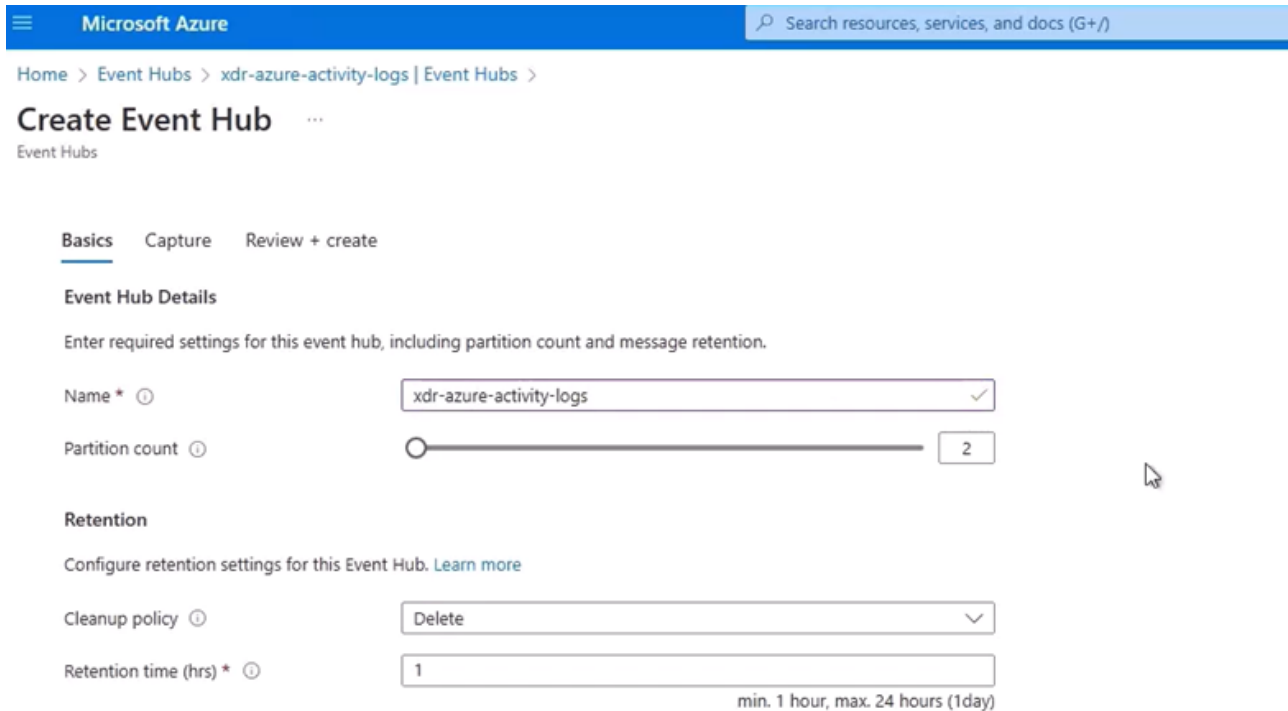
Showing 1 to 3 of 3 records.

Name	Status	Tier	Capacity	Location
xdr-azure-activity-logs	Active	Basic	1	East US
xdr-azure-audit-logs	Activating	Basic	1	East US
xdr-azure-sign-in-logs	Activating	Basic	1	East US

3. Click **Create Event Hub**.

We recommend the following naming convention:

- xdr-azure-activity-logs
- xdr-azure-audit-logs
- xdr-azure-sign-in-logs



Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Event Hubs > xdr-azure-activity-logs | Event Hubs >

## Create Event Hub

Event Hubs

Basics Capture Review + create

### Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name \* ⓘ xdr-azure-activity-logs ✓

Partition count ⓘ  2

### Retention

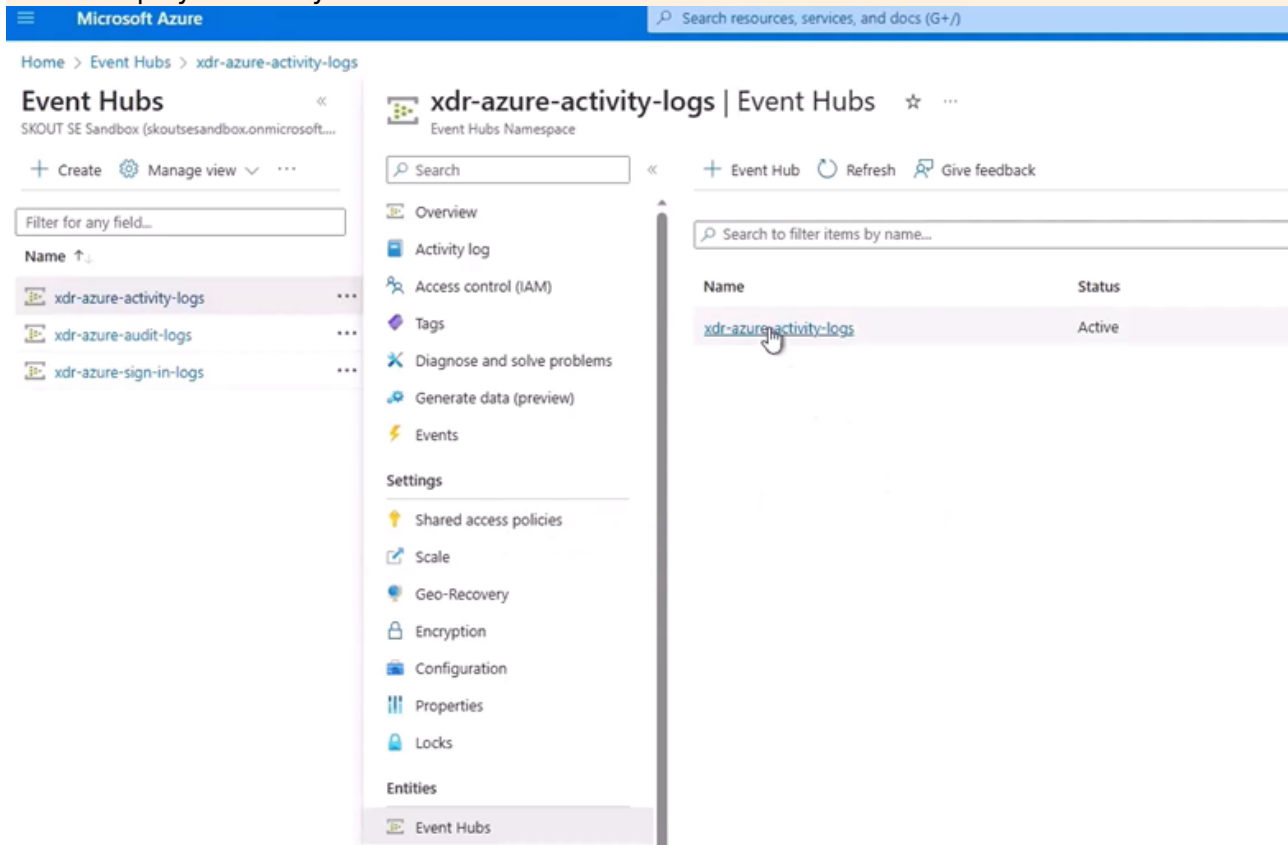
Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy ⓘ Delete

Retention time (hrs) \* ⓘ 1  
min. 1 hour, max. 24 hours (1day)

- Repeat steps 2-3 for the rest of the namespaces.
- Click **Review and Create**.

The deployment may take a while.



Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Event Hubs > xdr-azure-activity-logs

## Event Hubs

SKOUT SE Sandbox (skoutsandbox.onmicrosoft...)

+ Create Manage view ...

Filter for any field...

Name ↑

xdr-azure-activity-logs	...
xdr-azure-audit-logs	...
xdr-azure-sign-in-logs	...

### xdr-azure-activity-logs | Event Hubs

Event Hubs Namespace

Search

+ Event Hub Refresh Give feedback

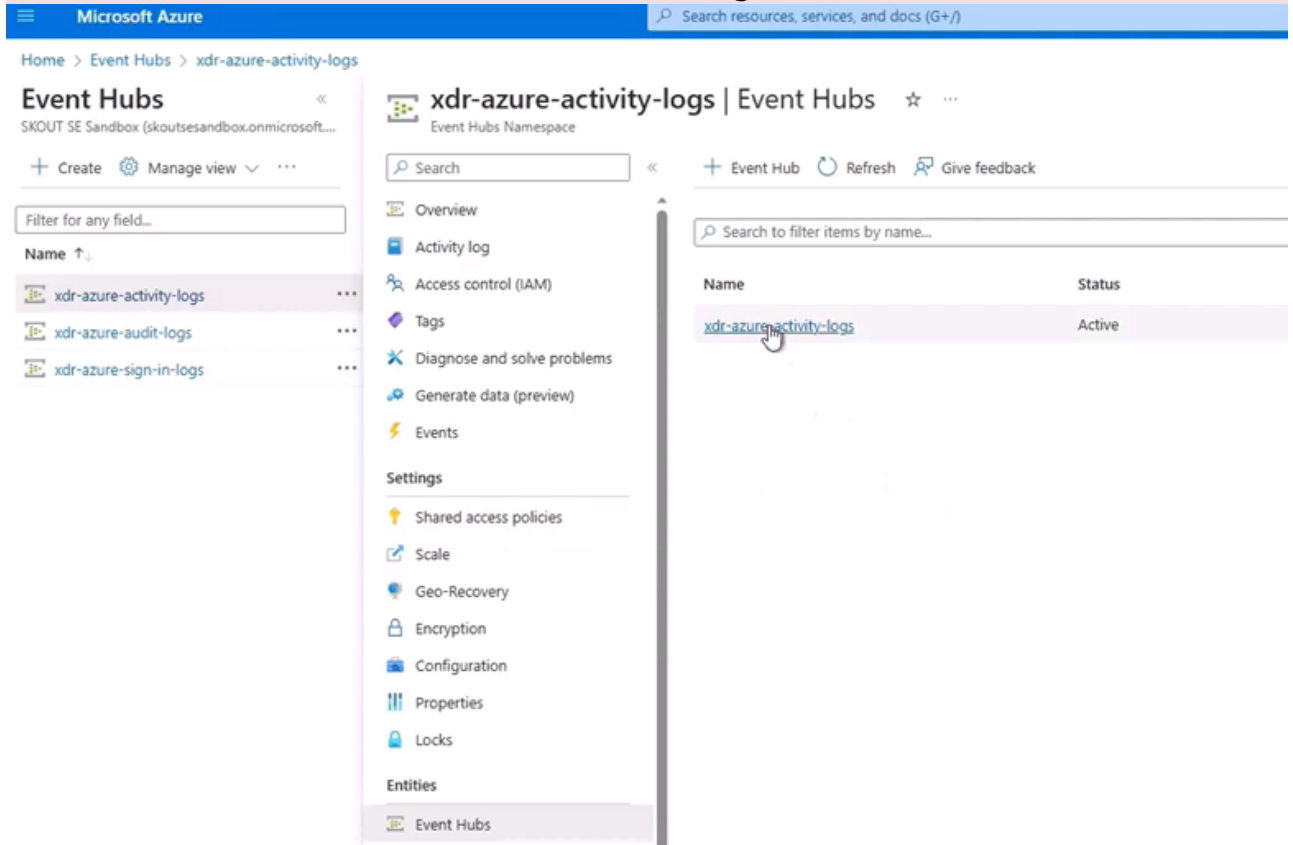
Search to filter items by name...

Name	Status
xdr-azure-activity-logs	Active

## To set up an Event Hub Shared Access Policy

1. In **Event Hubs**, on the right, click the link **Event Hub Namespace** that you created in the previous procedure.

Do not click **Shared Access Policies** under **Settings**.

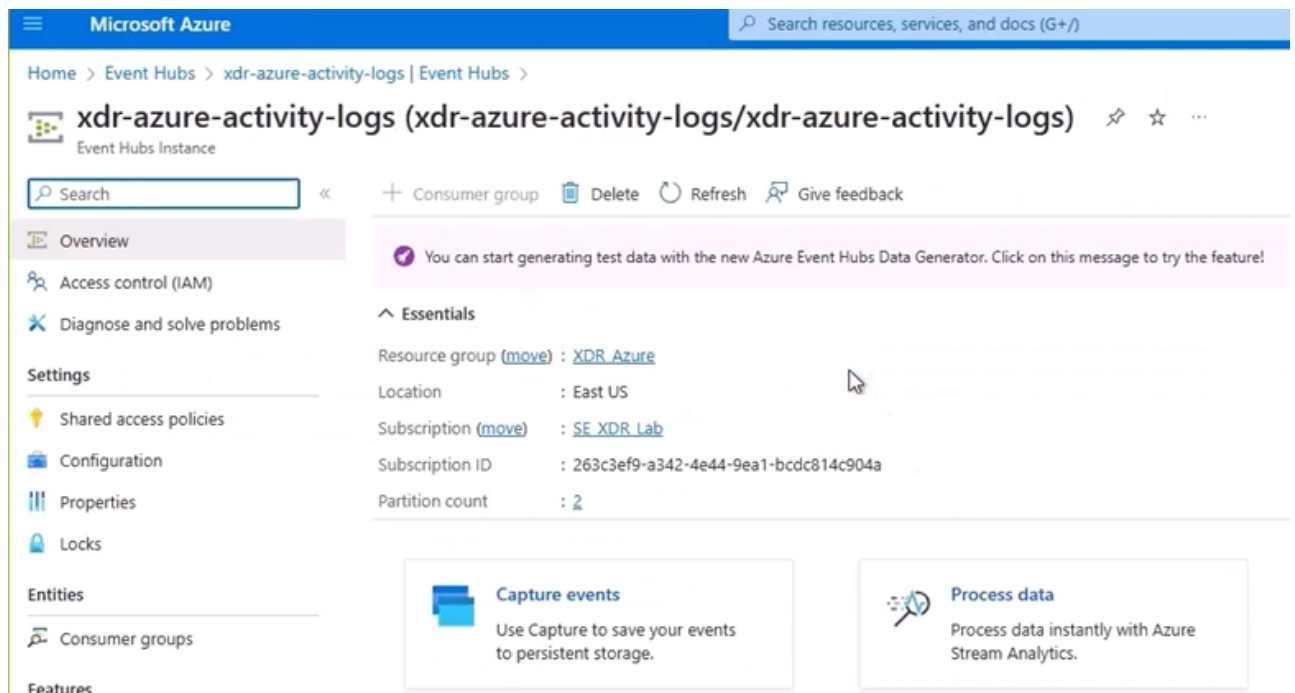


The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Microsoft Azure' logo and a search bar. The breadcrumb trail indicates the path: Home > Event Hubs > xdr-azure-activity-logs. The main content area is titled 'Event Hubs' and shows the 'xdr-azure-activity-logs' namespace. On the left, a list of event hubs is displayed, with 'xdr-azure-activity-logs' selected. On the right, a table shows the 'xdr-azure-activity-logs' namespace with a status of 'Active'. The 'Settings' section on the left includes 'Shared access policies', 'Scale', 'Geo-Recovery', 'Encryption', 'Configuration', 'Properties', 'Locks', and 'Entities'.

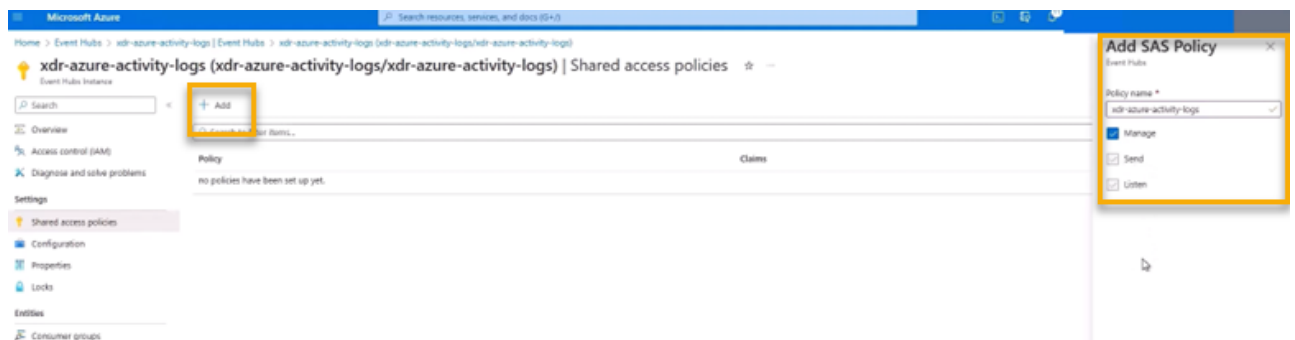
Name	Status
xdr-azure-activity-logs	Active

2. Click **Shared Access Policies**.





3. Click **Add**.



4. In **Add SAS Policy**, in **Policy Name**, type the name of the namespace.

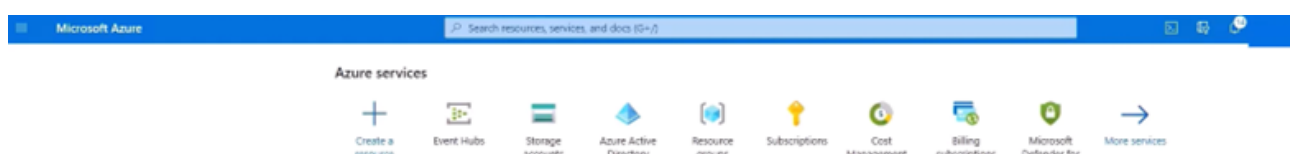
5. Select the **Manage** checkbox.

6. Repeat steps 1-5 for the rest of the namespaces.

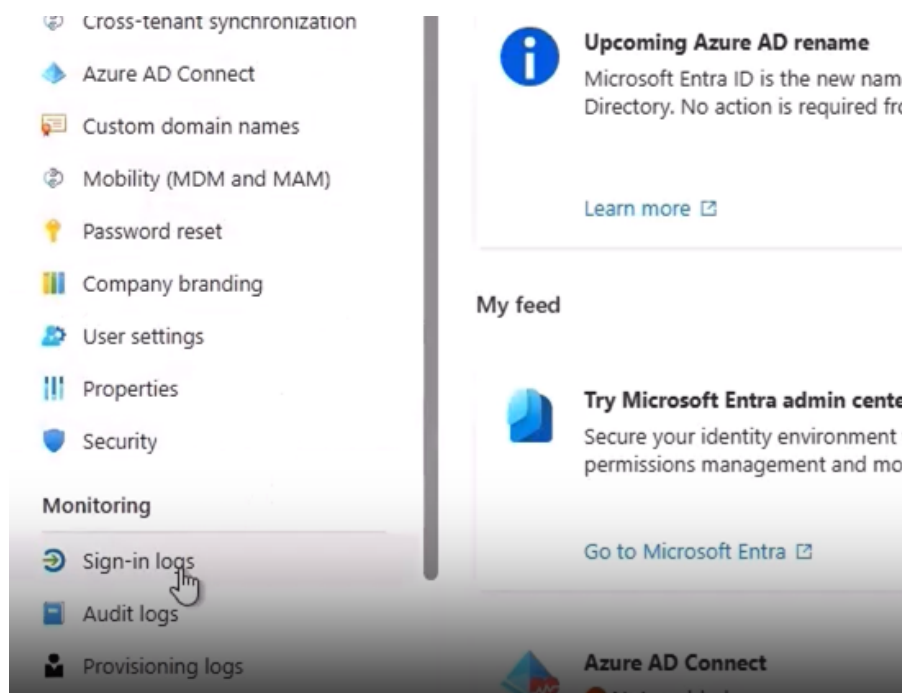
## Part 2: Updating Diagnostic Settings

To update diagnostic settings for the sign in log

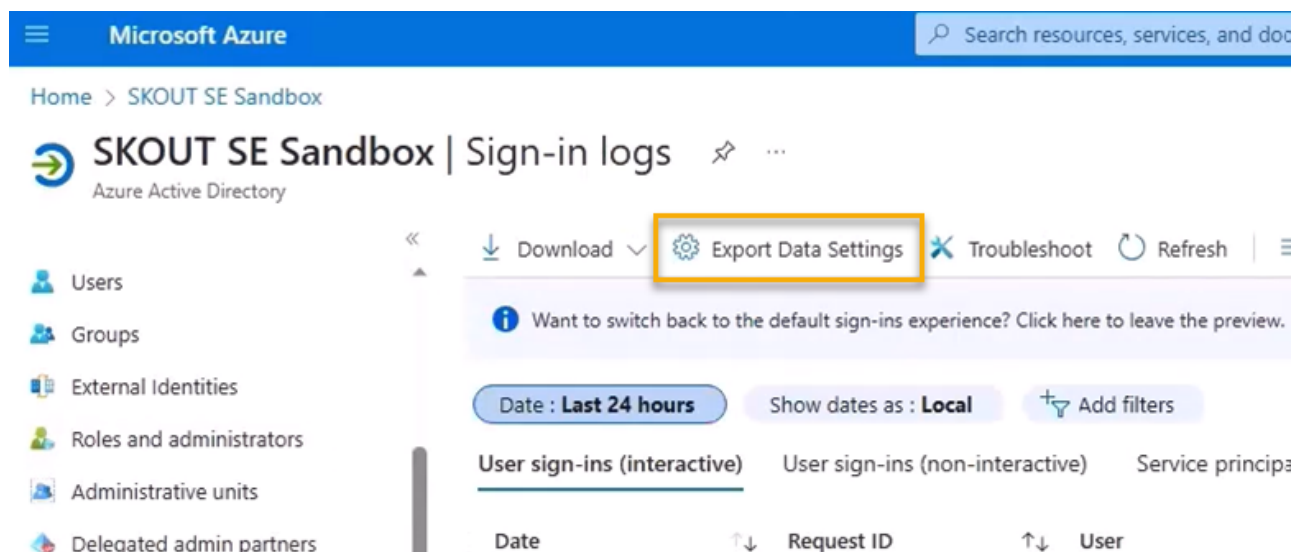
1. Navigate to **Azure Active Directory**.



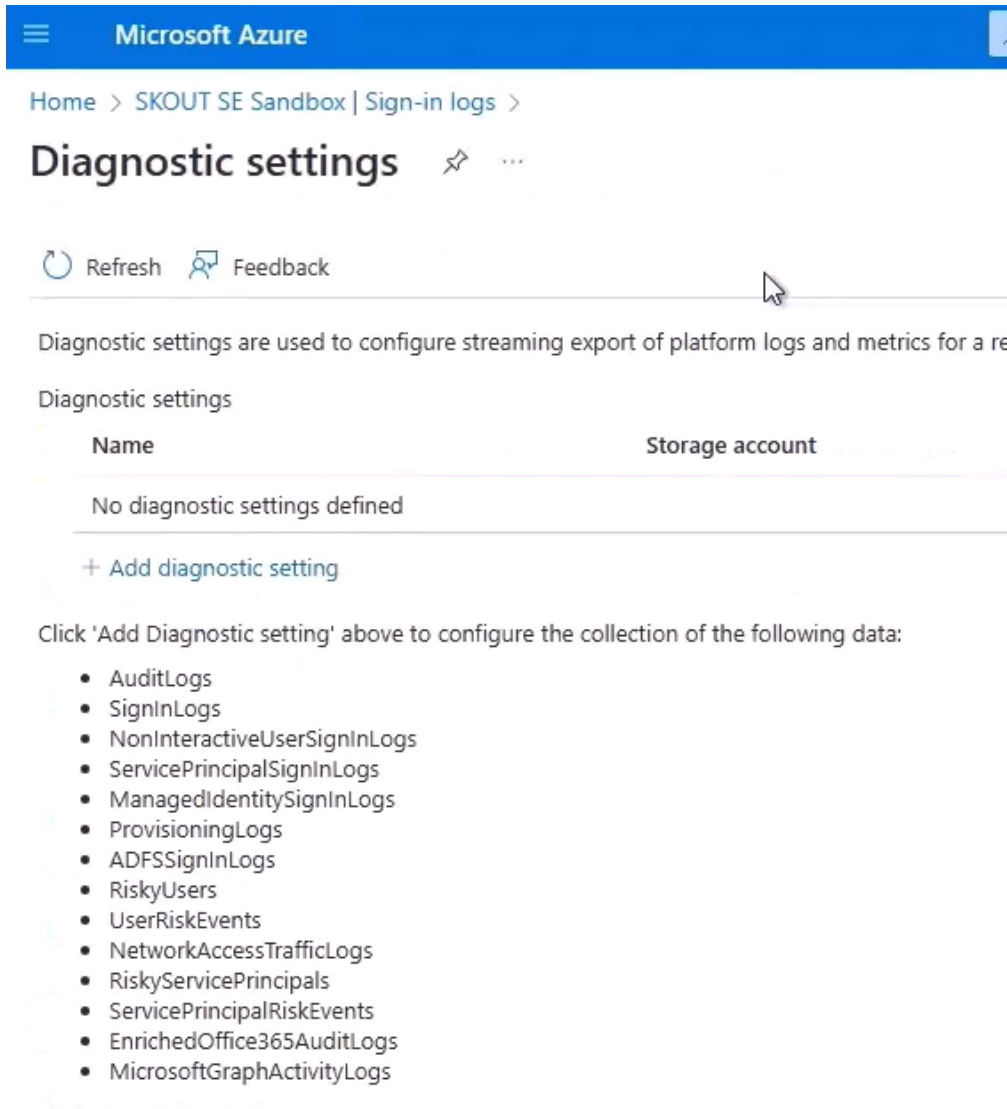
2. In the **Monitoring** section, click **Sign-in logs**.



3. Click **Export Data Settings**.



4. Click **Add diagnostic setting**.



Microsoft Azure

Home > SKOUT SE Sandbox | Sign-in logs >

## Diagnostic settings

Refresh Feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource.

Diagnostic settings

Name	Storage account
No diagnostic settings defined	

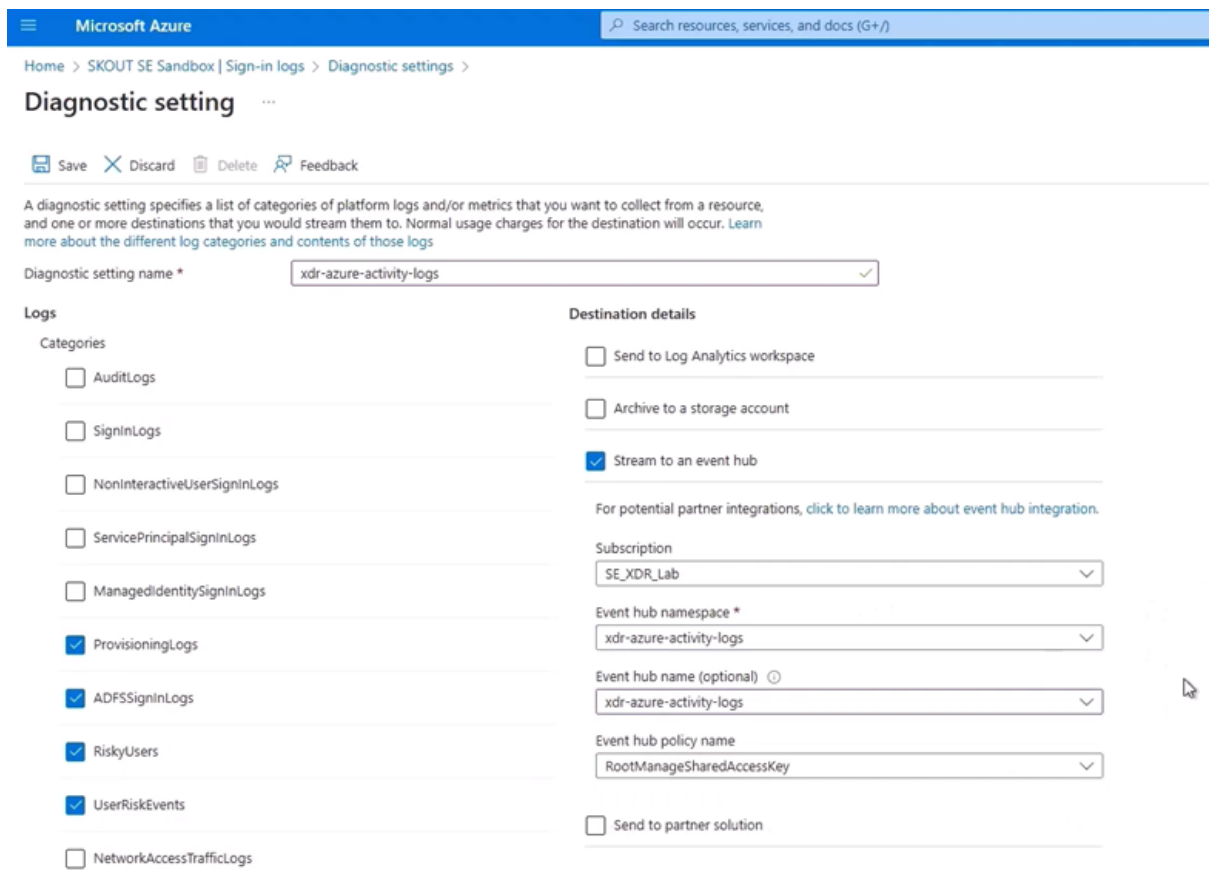
[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- ☐ AuditLogs
- ☐ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs
- ☐ RiskyServicePrincipals
- ☐ ServicePrincipalRiskEvents
- ☐ EnrichedOffice365AuditLogs
- ☐ MicrosoftGraphActivityLogs

5. Do the following:

- In **Diagnostic setting name**, type the name of your sign in log.
- Select the following checkboxes:
  - **SignInLogs**
  - **NonInteractiveUserSignInLogs**
  - **ServicePrincipleSignInLogs**
  - **ManagedIddentitySignInLogs**
  - **Stream to an event hub**
- Select the correct **Subscription and Event hub namespace** (Ex: xdr-azure-sign-in-logs).

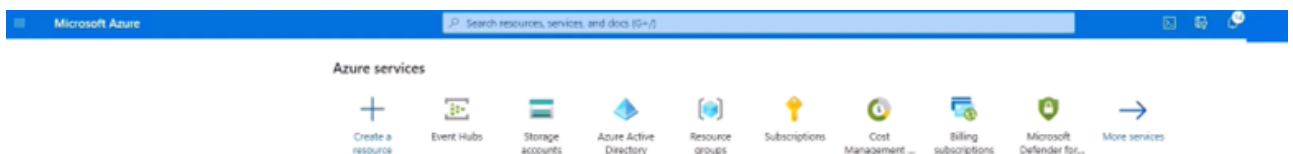


The screenshot shows the 'Diagnostic setting' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > SKOUT SE Sandbox | Sign-in logs > Diagnostic settings > Diagnostic setting'. The page title is 'Diagnostic setting'. Below the title are buttons for 'Save', 'Discard', 'Delete', and 'Feedback'. A description states: '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'. The 'Diagnostic setting name' is 'xdr-azure-activity-logs'. Under the 'Logs' section, the 'Categories' list includes 'AuditLogs', 'SignInLogs', 'NonInteractiveUserSignInLogs', 'ServicePrincipalSignInLogs', 'ManagedIdentitySignInLogs', 'ProvisioningLogs' (checked), 'ADFSSignInLogs' (checked), 'RiskyUsers' (checked), 'UserRiskEvents' (checked), and 'NetworkAccessTrafficLogs'. Under the 'Destination details' section, 'Send to Log Analytics workspace' and 'Archive to a storage account' are unchecked, while 'Stream to an event hub' is checked. A link says 'For potential partner integrations, click to learn more about event hub integration.' The 'Subscription' is 'SE\_XDR\_Lab'. The 'Event hub namespace' is 'xdr-azure-activity-logs'. The 'Event hub name (optional)' is 'xdr-azure-activity-logs'. The 'Event hub policy name' is 'RootManageSharedAccessKey'. 'Send to partner solution' is unchecked.

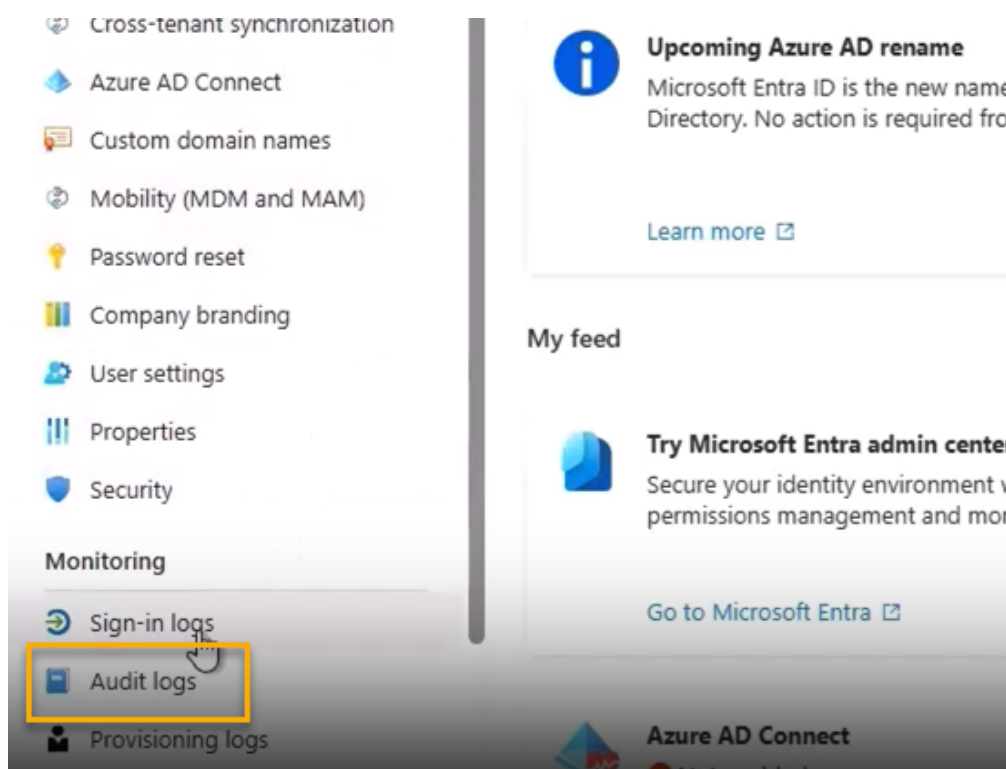
6. Click **Save**.

To update diagnostic settings for for the audit log and activity log

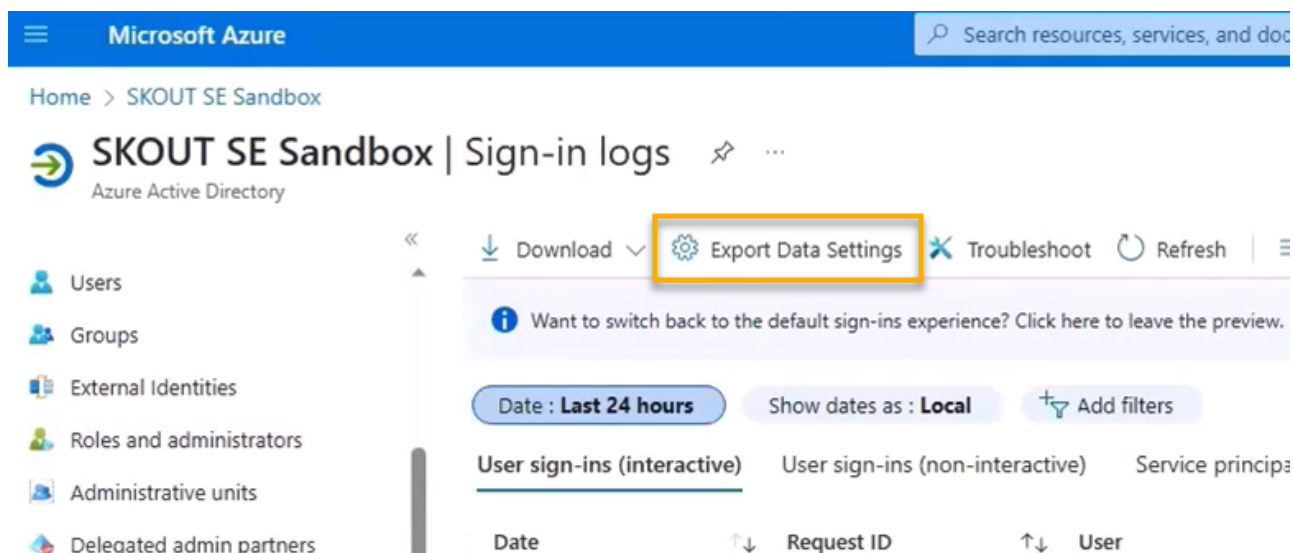
1. Navigate to **Azure Active Directory**.



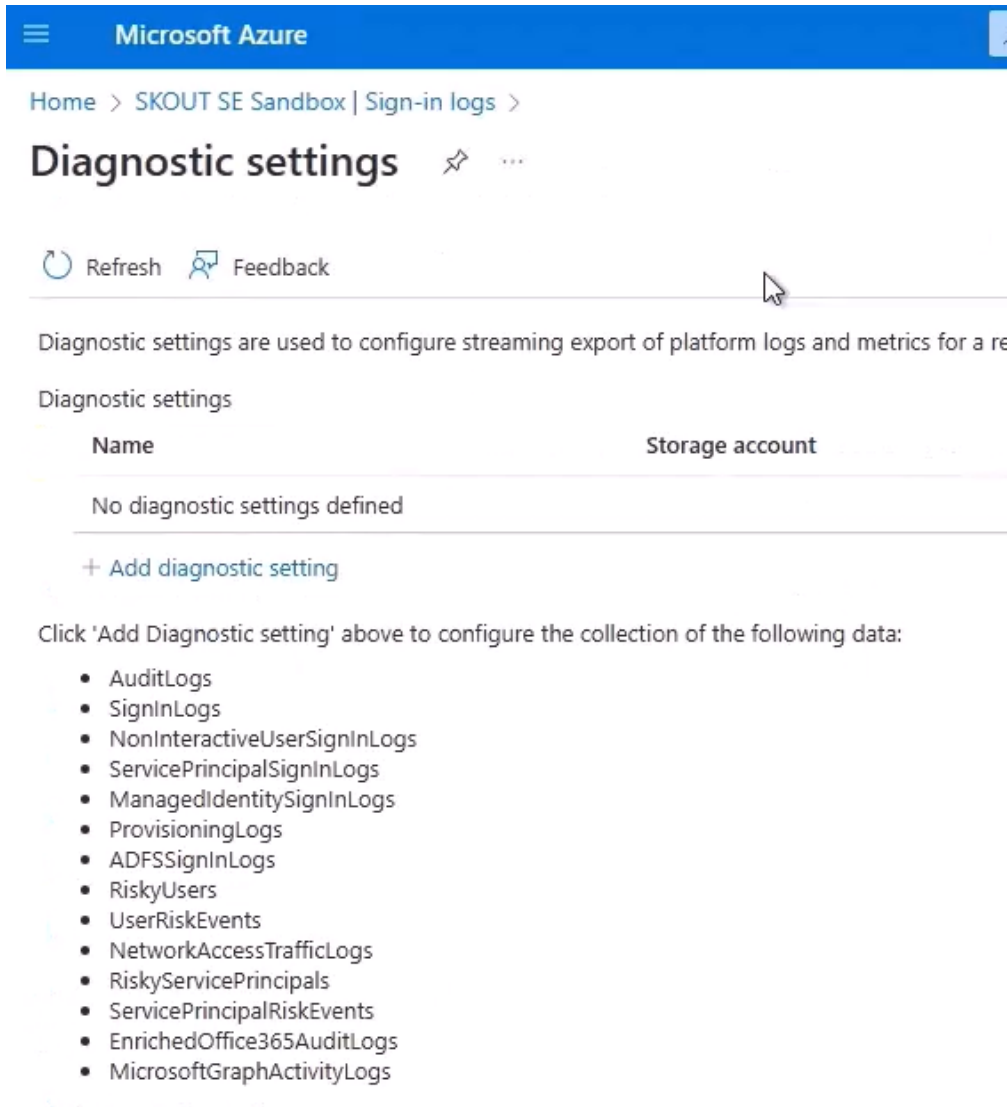
2. In the **Monitoring** section, click **Audit logs**.



3. Click **Export Data Settings**.



4. Click **Add diagnostic setting**.



Microsoft Azure

Home > SKOUT SE Sandbox | Sign-in logs >

## Diagnostic settings

Refresh Feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource.

Diagnostic settings

Name	Storage account
No diagnostic settings defined	

[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- ☒ AuditLogs
- ☒ SignInLogs
- ☒ NonInteractiveUserSignInLogs
- ☒ ServicePrincipalSignInLogs
- ☒ ManagedIdentitySignInLogs
- ☒ ProvisioningLogs
- ☒ ADFSSignInLogs
- ☒ RiskyUsers
- ☒ UserRiskEvents
- ☒ NetworkAccessTrafficLogs
- ☒ RiskyServicePrincipals
- ☒ ServicePrincipalRiskEvents
- ☒ EnrichedOffice365AuditLogs
- ☒ MicrosoftGraphActivityLogs

5. Do the following:

- In **Diagnostic setting name**, type the name of your audit log namespace.
- Select the following checkboxes:
  - **AuditLogs**
  - **Stream to an event hub**
- Select the correct **Subscription and Event hub namespace** (Ex: xdr-azure-audit-logs).

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > SKOUT SE Sandbox | Sign-in logs > Diagnostic settings >

### 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 \*

#### Logs

Categories

☒ AuditLogs

☐ SignInLogs

☐ NonInteractiveUserSignInLogs

☐ ServicePrincipalSignInLogs

☐ ManagedIdentitySignInLogs

☐ ProvisioningLogs

☐ ADFSSignInLogs

☐ RiskyUsers

☐ UserRiskEvents

☐ NetworkAccessTrafficLogs

#### Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

Event hub namespace \*

Event hub name (optional)

Event hub policy name

☐ Send to partner solution

6. Click **Save**.
7. Repeat steps 1-6 for the activity log.

Home > SKOUT SE Sandbox | Sign-in logs >

### Diagnostic settings

Refresh

Feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace
xdr-azure-activity-logs	-	xdr-azure-activity-logs/xdr-azure-activity-logs	
xdr-azure-audit-logs	-	xdr-azure-audit-logs/xdr-azure-audit-logs	
xdr-azure-sign-in-logs	-	xdr-azure-sign-in-logs/xdr-azure-sign-in-logs	

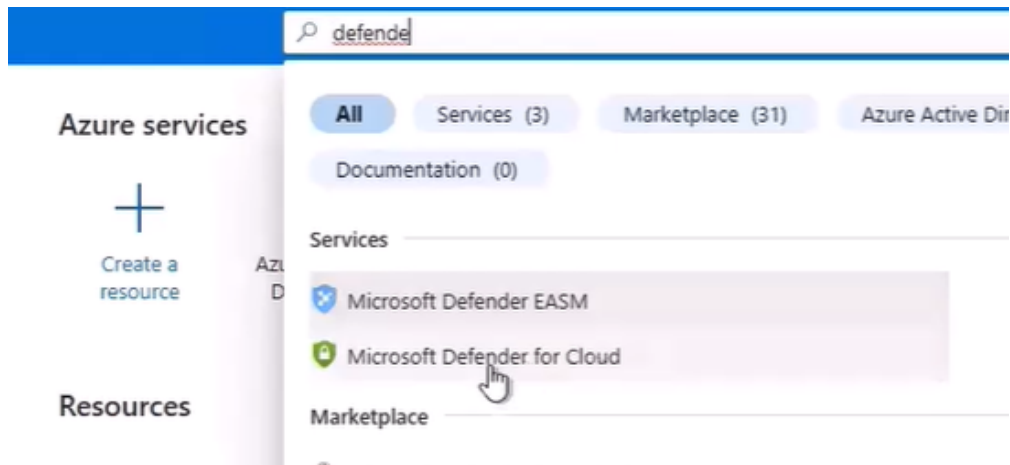
[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

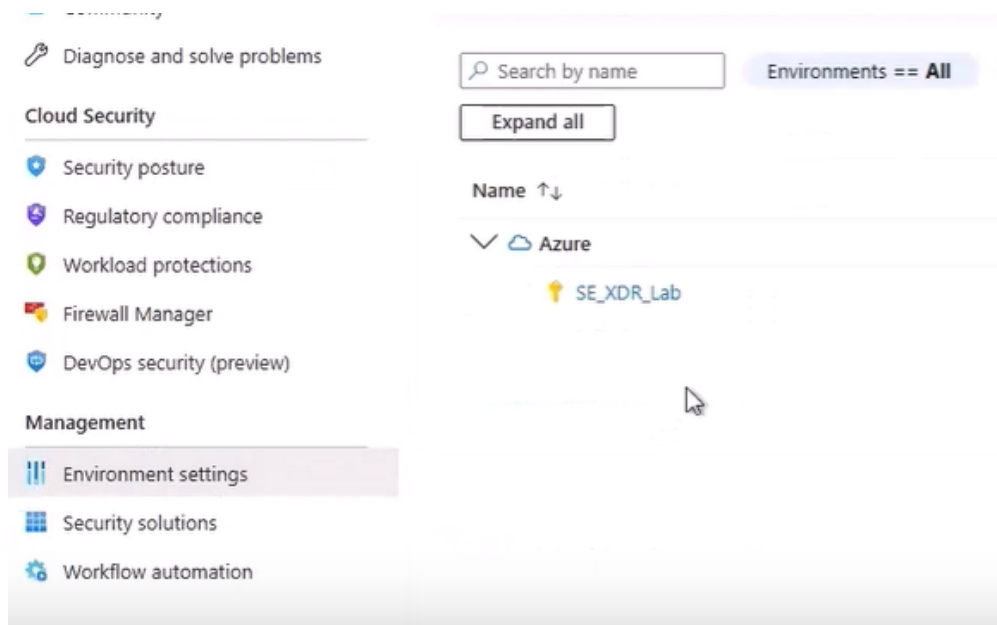
- AuditLogs
- SignInLogs

To set up Microsoft Defender for Cloud

1. Navigate to **Microsoft Defender for Cloud**.



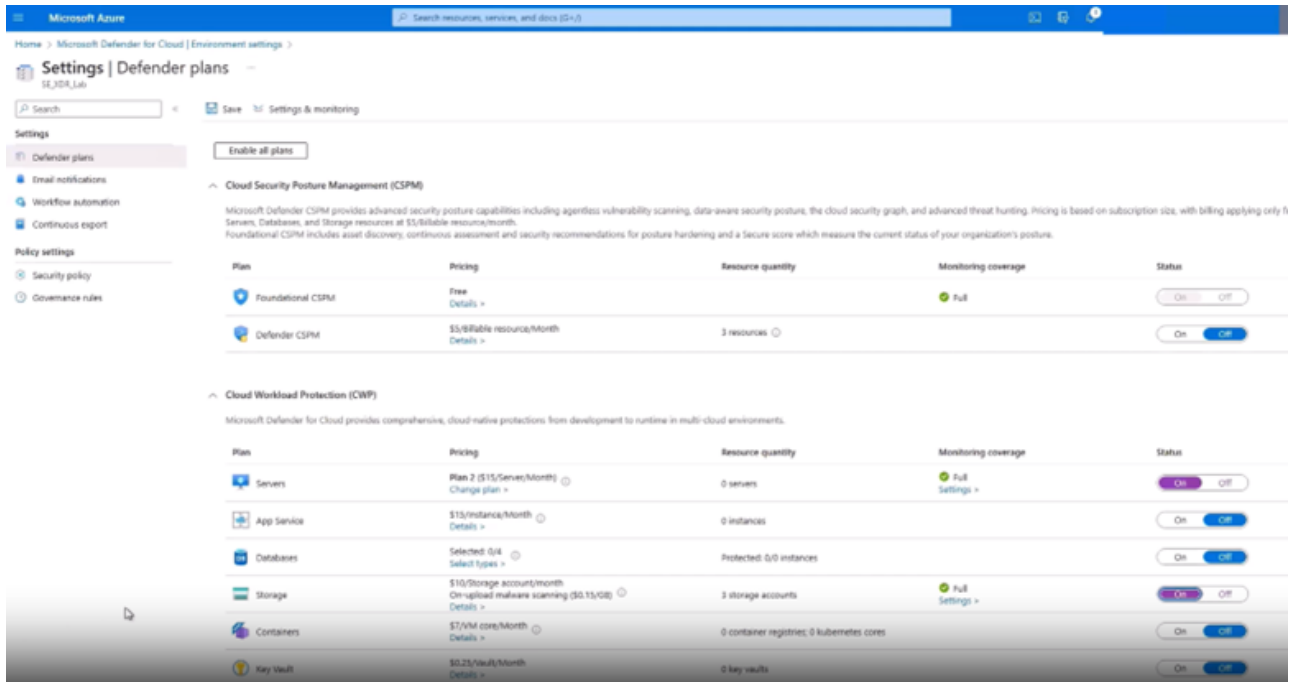
2. Under **Management**, click **Environment settings**.



3. Select your subscription.

4. If you're setting up for the first time, set **Severs** and **Storage** to **On**, then click **Save**.





The screenshot shows the Microsoft Defender for Cloud settings page. The left sidebar contains the following sections:

- Settings**
  - Defender plans
  - Email notifications
  - Workflow automation
  - Continuous export
- Policy settings**
  - Security policy
  - Governance rules

The main content area is titled "Settings | Defender plans" and includes a search bar, a "Save" button, and a "Settings & monitoring" link. Below this, there are two main sections:

### Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only to Servers, Databases, and Storage resources at \$5/billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free <a href="#">Details &gt;</a>		Full	On <input type="checkbox"/> Off <input type="checkbox"/>
Defender CSPM	\$5/billable resource/Month <a href="#">Details &gt;</a>	3 resources		On <input type="checkbox"/> Off <input checked="" type="checkbox"/>

### Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) <a href="#">Change plan &gt;</a>	0 servers	Full <a href="#">Settings &gt;</a>	On <input type="checkbox"/> Off <input type="checkbox"/>
App Service	\$15/instance/Month <a href="#">Details &gt;</a>	0 instances		On <input type="checkbox"/> Off <input checked="" type="checkbox"/>
Databases	Selected SQL Default types >	Protected: 0/0 instances		On <input type="checkbox"/> Off <input checked="" type="checkbox"/>
Storage	\$10/Storage account/Month On-upload malware scanning (\$0.15/GB) <a href="#">Details &gt;</a>	3 storage accounts	Full <a href="#">Settings &gt;</a>	On <input type="checkbox"/> Off <input type="checkbox"/>
Containers	\$7/VM core/Month <a href="#">Details &gt;</a>	0 container registries; 0 Kubernetes cores		On <input type="checkbox"/> Off <input checked="" type="checkbox"/>
Key Vault	\$0.25/secret/Month <a href="#">Details &gt;</a>	0 key vaults		On <input type="checkbox"/> Off <input checked="" type="checkbox"/>

5. Under the **Settings** section, click **Continuous Exports**.
6. Do the following:
7. Select the **Security recommendations** checkbox, and select **All recommendations**.
8. In **Security Alerts**, select **Low, Medium, High, Informational**.
9. Turn **Streaming Updates** on.
10. Turn **Snapshots** off.
11. In **Export configuration**, select your subscription.

## Export configuration

Resource group \* ⓘ

XDR\_Azure ▼

12. In **Export Target**, do the following:
  - In **Subscription**, select your subscription
  - In **Event Hub namespace**, select the name of your activity log.
  - In **Event Hub name**, select the name of your activity log.
  - In **Event hub policy name**, select the name of your activity log.

**Export target**☐ Export as a trusted service ⓘ

Subscription \*

SE\_XDR\_Lab

Event Hub namespace \*

xdr-azure-activity-logs

Event Hub name \*

xdr-azure-activity-logs

Event hub policy name \*

xdr-azure-activity-logs

13. Click **Save**.

### Part 3: Barracuda XDR Dashboard Setup for Microsoft Azure

#### To set up Barracuda XDR Dashboard Setup for Microsoft Azure

1. In Azure, click **Event Hubs**, then click one of the activity logs.
2. Click **Event Hubs**, then click the link of the log.
3. Click **Shared access policies**.
4. In the right side, copy the **Connection string-primary key**.
5. Open another browser tab and start **Barracuda XDR Dashboard**.
6. In **Barracuda XDR Dashboard**, click **Setup > Integrations**.
7. On the **Microsoft Azure** card, click **Setup**.
8. Select the **Enabled** checkbox.
9. In the **Activity Log** section, do the following:
10. In **Event Hub**, type the name of the **Activity Log**.
11. In **Connection String**, paste the **Connection string-primary key**.
12. In **Azure**, click **Home, Storage Accounts**.
13. Click the link of the Activity Log.
14. Copy the name of the Storage Account.
15. In **Barracuda XDR Dashboard**, in **Storage Account**, paste the name of the Storage Account.
16. In **Azure**, click **Access Keys**.
17. In the **key1** section, copy the Key.
18. In **Barracuda XDR Dashboard**, in **Storage Account Key**, paste the key.
19. Repeat steps 1-19 for the rest of the logs.
20. Click **Save**.



## Figures

3. EventHubNamespaces.png
4. CreateNamespaces.png
5. ListofEventHubs.png
6. CreateStorage Account.png
7. StorageAccounts.png
8. EvenHubEntity.png
9. CreateEventHub.png
10. EventHubs4.png
11. EventHubs3.png
12. ActivityLogsSettings.png
13. AddSAS.png
14. AzureActiveDirectory.png
15. SignInLogs.png
16. ExportDataSettings.png
17. DiagnosticSettings.png
18. DiagnosticSettings4.png
19. AzureActiveDirectory.png
20. AuditLogs.png
21. ExportDataSettings.png
22. DiagnosticSettings.png
23. DiagnosticSettings3.png
24. DiagnosticSettings5.png
25. DefenderForCloud.png
26. DefenderForCloud2.png
27. DefenderForCloud3.png
28. ExportConfiguration.png
29. ExportTarget.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.