Cloud Connections

This topic only applies to **Armor Anywhere** users.

To fully use this screen, you must add the following permissions to your account:

- Read Cloud Connections
- Write Cloud Connections

Overview

You can use the **Cloud Connections** screen to sync your public cloud account into the Armor Management Portal (AMP). Afterwards, you can use AMP to:

- Collect and store logs with the **Host Log Collector** add-on product
  - To specifically collect CloudTrail logs, see Collect and view CloudTrail logs in AMP.
- View the security status of your instance in the **Virtual Machines** screen

  While all instances from your public cloud account will appear in the **Virtual Machines** screen, you should only focus on the security status for the instances that contain the Armor agent.

- Add AWS Security Hub feature to your public cloud account.

Currently, the **Cloud Connections** screen supports Amazon Web Services (AWS).

You can use this screen to collect CloudTrail logs and EC2 instance logs.

Review Cloud Connections screen

The **Cloud Connections** screen displays the public cloud accounts you have synced.

Column	Description
Account Name	This column displays the descriptive name for your account. You can also click the arrow to see which Armor services are associated with the account.
Provider	This column displays the public cloud provider.
Account ID	This column displays the ID for your public cloud account.
Status	This column displays the connection status between your Armor accounts and your public cloud account.

Add an AWS public cloud account

You can use the **Cloud Connections** screen to sync your public cloud environment into the Armor Management Portal (AMP).

In this section, you will need to access your AWS console to complete the configuration process.

> Armor will generate an **External ID** for every new Cloud Connection account. As result, an incomplete cloud connection account will be listed in the table as **(Pending Connection)**. You can click this entry in order to continue with the cloud connection creation process.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Cloud Connections**.
3. Click the plus (+) icon.
4. In **Account Name**, enter a descriptive name.
5. In **Description**, enter a short description.
6. In **Services**, select the data type to collect.
    - To collect CloudTrail logs, you must have the Log Depot add-on product enabled.
        - To learn how to enable Log Depot, see Collect host-based logs through Log Relay (Armor Anywhere).
        - To learn how to collect CloudTrail logs, see Collect and view CloudTrail logs in AMP.
7. In **IAM Role**, copy the **External ID**. You will need this information at a later step.
    - The **Armor's AWS Account Number** and **External ID** fields are pre-populated.
    - Armor will generate an **External ID** for every new Cloud Connection you create.
    - In a later step, you will locate the information to complete the **IAM Role ARN** field.
8. Access the AWS console.
9. Under **Security, Identity & Compliance**, click **IAM**.
10. In the left-side navigation, click **Roles**.
11. Click **Create role**.
12. Under **Select role type**, select Another AWS account.
13. In **Account ID**, enter **679703615338**.
14. Mark **Require external ID**.
15. In field that appears, paste the **External ID** you copied earlier from the Armor Management Portal (AMP).
16. Do not mark **Require MFA**.
17. Click **Next: Permissions**.
18. Locate and mark the **Security Audit** policy.
19. Locate and mark the **Security Hub Full Access** policy.
20. Click **Next: Review**.
21. In **Role name**, enter a descriptive name.
22. In **Role description**, enter a useful description.
23. Click **Create role**.
24. Locate and select the newly created role.
25. Under **Summary**, copy the **Role ARN** information.
26. Return to the **Cloud Connections** screen in AMP.
27. Paste the **Role ARN** information into the **IAM Role ARN** field.
28. Click **Save Cloud Connection**.
    - Once the newly added cloud connections begins to gather data, the instance will appear in the **Virtual Machines** screen.

View your added (connected) public cloud instances

After you add your public cloud account into the Armor Management Portal (AMP), you can view the corresponding instances (and their security status) in the **Virtual Machines** screen.

> The **Cloud Connection** screen simply lists the synced public cloud account; the **Virtual Machines** screen lists all the instances listed in that public cloud account.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.

Column	Description
Name	The name of the instance from your public cloud account
Type	The type of instance, specific to the offerings offered by your public cloud provider, such as en EC2 instance for AWS
Provider	The public cloud provider for the instance
OS	The operating system associated with the instance (For AWS, the associated AMI is listed)

Date Created	The date the instance was created in your public cloud account
Security Group	The security group that corresponds to your AWS instance. • This column will only appear to AWS users. • This column will only appear if you have selected the EC2 Metadata and orchestration option.
Keypair	The keypair that corresponds to your AWS instance. • This column will only appear to AWS users. • This column will only appear if you have selected the **EC2 Metadata and orchestration** option in the **Cloud Connections** screen..
State	The security status of the instance, in relation to the installed agent. There are three states: • **Unprotected** indicates the agent is not installed in the instance. • **Needs Attention** indicates that the agent is installed, but has not properly communicated (heartbeated) with Armor. • **OK** indicates that the agent is installed and has communicated (hearbeated) with Armor.
Power	The power status of the instance, either powered on (green) or powered off (red)

Review API Keys

- Post Cloud Connections
- Delete Cloud Connections
- Get Cloud Connections
- Get Cloud Connections (Status)
- Get Cloud Connections (Service Types)

Troubleshoot Cloud Connections screen

If you do not see any data in the **Cloud Connections** screen, consider that:

- You do not have permission to view log data.
  - You must have the **Read Cloud Connections** and **Writer Cloud Connections** permissions enabled to view log data. Contact your account administrator to enable this permission. To learn how to update you permissions, see Roles and Permissions (Armor Complete).