Create a Cloud Connection for AWS Security Hub

Armor Knowledge Base

Topics Discussed

- Review Pre-Deployment Considerations
- Create a Cloud Connection account for AWS

To fully use this feature, you must have the following permissions in your account:

- Read Cloud Connections
- Write Cloud Connections

You can use these instructions to sync your AWS account with your AMP account. Specifically, this action will sync your AMP account with AWS Security Hub where Armor will send security updates.

To complete these instructions, you must be able to access your AWS console.

Review Pre-Deployment Considerations

Before you configure your AMP and AWS account, review the following pre-deployment considerations:

Security Findings

When you sync your AMP account with AWS Security Hub, Armor will send the following information to AWS Security Hub:

Security data	Description	Number of security findings
Malware	In relation to **malware**, Armor communicates with AWS Security Hub on an hourly basis. If Armor detects a malware event, this information will be sent to AWS Security Hub within an hour. To learn more about Malware Protection, see ANYWHERE Malware Protection.	The number of security findings is based on the number of virtual machines, as well as the security posture of those virtual machines. Malware is a seldom event, with only a couple events reported per day.
Vulnerability Scanning	In relation to **vulnerability scanning**, Armor communicates with AWS Security Hub on a weekly basis. If Armor detects a vulnerability, this information will be sent to AWS Security Hub within a week. For vulnerabilities, Armor will only send vulnerabilities that are **critical** or **high**, based on the CVSS scoring structure. In these cases, Armor will only send vulnerabilities that contain a score of 5.5 or higher. To learn more about Vulnerability Scanning, see ANYWHERE Vulnerability Scanning.	The number of security findings is based on the number of virtual machines, as well as the security posture of those virtual machines. For large enterprise customers, the number of vulnerabilities can range from 100 to 1,000 within a weekly time frame.

Exchanging Account Information

To properly sync your AMP account with AWS, the Armor AWS Account will assume a role in your AWS account. To accomplish this, in AMP you will copy the Armor AWS account number and a unique external ID, and then paste into your AWS account. Afterwards, you will receive an AWS-generated ARN from the role, which you will then paste into AMP.

ASFF Types

The following table describes the ASFF-formatted finding types for the security finding that are sent to AWS Security Hub.

Finding	Types.Namespace	Types.Category	Types.Classifier
Vulnerability	Software configurations and checks	CVE	Dynamic based on CVE (i.e. CVE-2018-2771)
Malware	TTPs	N/A	N/A

Scoring Types

The following table describes the Severity.Product scores and the Severity.Normalized scores for the security findings that are sent to AWS Security Hub.

Finding	Severity.Product	Severity.Normalized	Notes
Vulnerabilities	While scores 0 - 10 are available to be sent, currently, Armor will only send scores 5.5 and higher.	While scores 0 - 30 are available, Armor will only send scores 5.5 and higher (5.5 * 3)	Calculation: CVSS score * 3. Armor will only send **critical** and **high** scores.
Malware	Scores 0 -10 is available.	Scores 31 - 61 are available.	Calculation: (Severity score * 3) + 31

Updated Fields for Findings

The following fields will be updated:

- The **recordState** will change to archived if the vulnerability or malware is no longer valid.
- The **updatedAt** will reflect the most recent timestamp that the finding was updated.

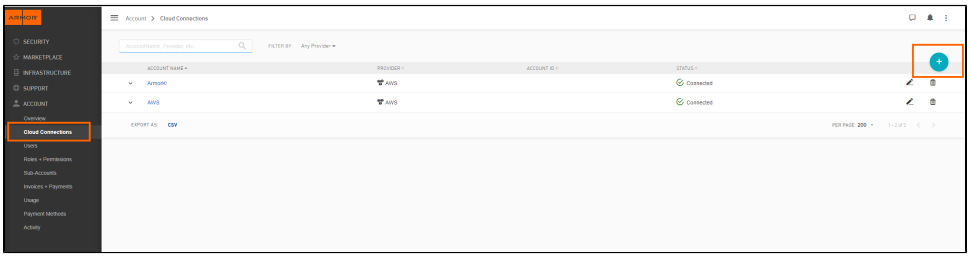
Create a Cloud Connection account for AWS

To complete these instructions, you must be able to access your AWS console.

> ⚠ 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.

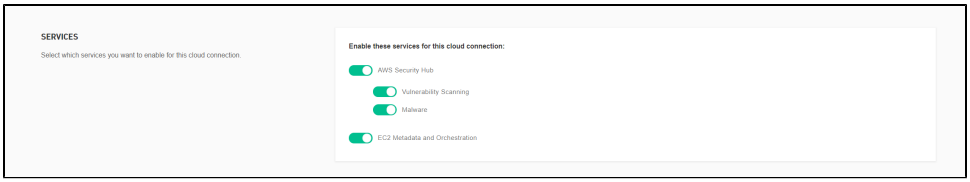
Step 1: Add your AWS account to AMP

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Account**.
2. Click **Cloud Connections**.
3. Click the plus (+) icon.

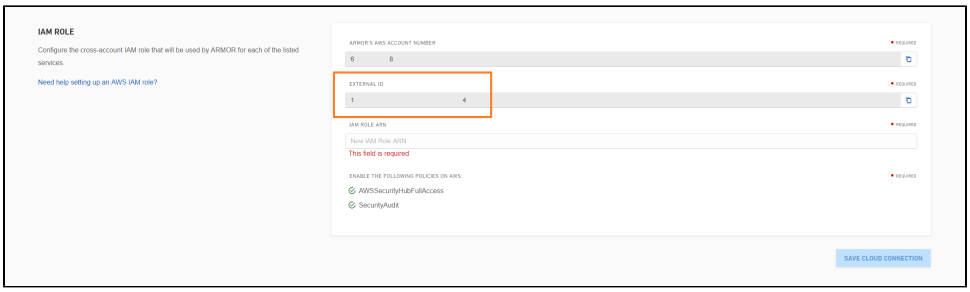


4. In **Account Name**, enter a descriptive name.
5. In **Description**, enter a short description.

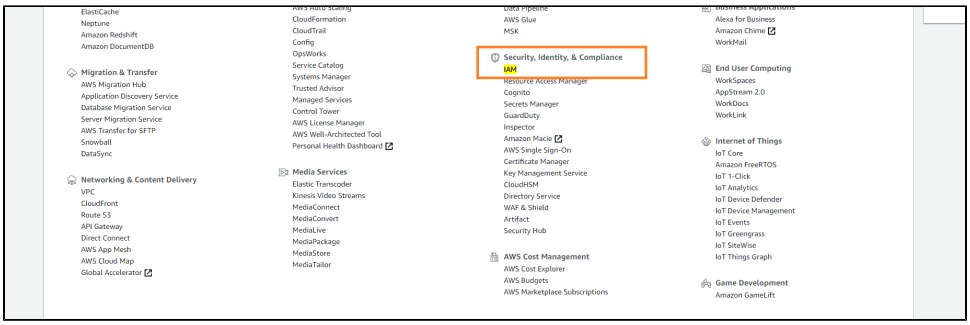
6. In **Services**, select the desired services.
    - To have Armor send security findings to your AWS Security Hub, mark **Security Hub.**
        - This action will automatically select additional services; these services must be selected.



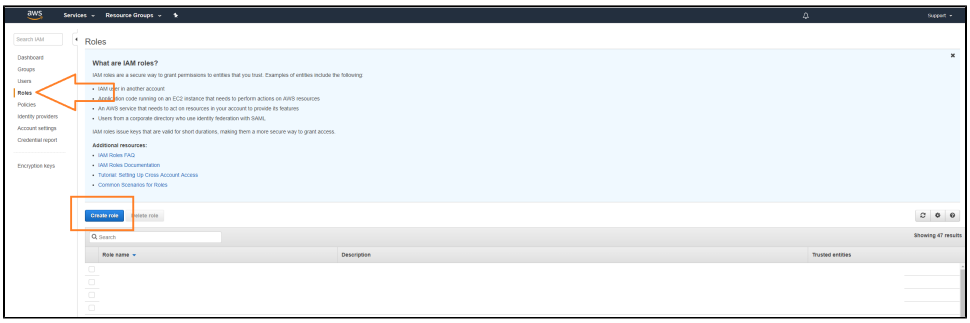
7. In **IAM Role**, copy the **External ID**. You will need this information at a later step.
    - The **Armor's AWS Account Number** and **External ID** fields are pre-populated.
    - Armor will generate an **External ID** for every new Cloud Connection you create.
    - In a later step, you will locate the information to complete the **IAM Role ARN** field.



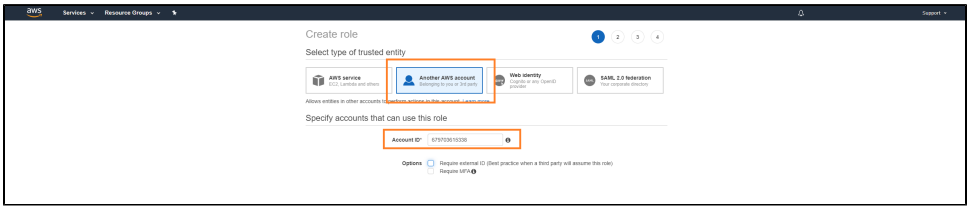
8. Access the AWS console.
9. Under **Security, Identity & Compliance**, click **IAM**.



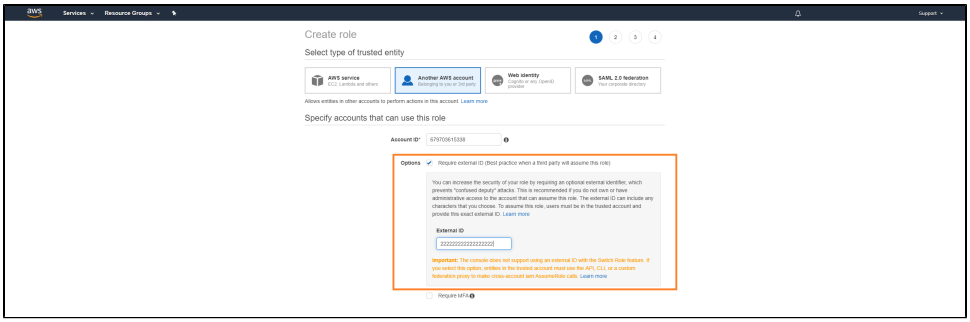
10. In the left-side navigation, click **Roles**.
11. Click **Create role**.



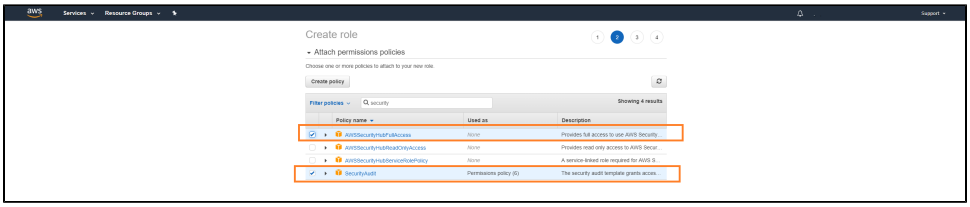
12. Under **Select role type**, select **Another AWS account**.
13. In **Account ID**, enter **679703615338**.



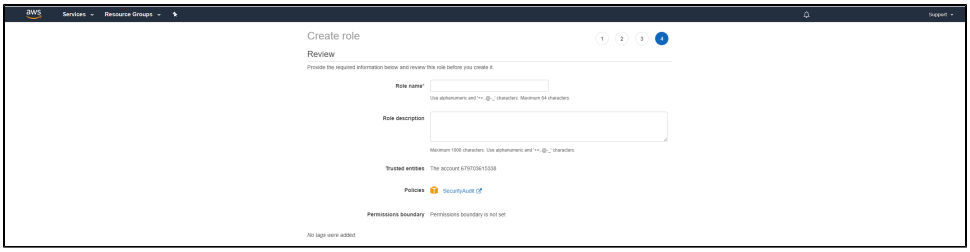
14. Mark **Require external ID**.
15. In field that appears, paste the **External ID** you copied earlier from the Armor Management Portal (AMP).



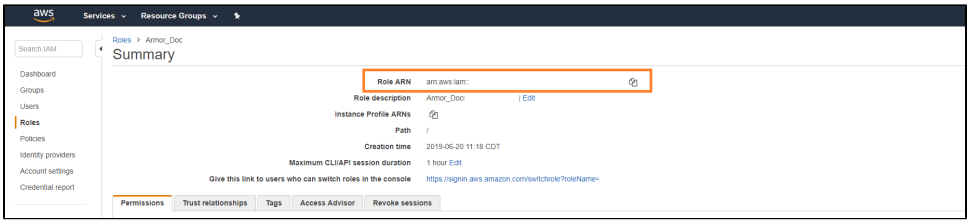
16. Do not mark **Require MFA**.
17. Click **Next: Permissions**.
18. Locate and mark the **SecurityAudit** policy.
19. Locate and mark the **AWSSecurityHubFullAccess** policy.



20. Click **Next: Tags**.
21. Click **Next: Review**.
22. In **Role name**, enter a descriptive name.
23. In **Role description**, enter a useful description.



24. Click **Create role**.
25. Locate and select the newly created role.
26. Under **Summary**, copy the **Role ARN** information.

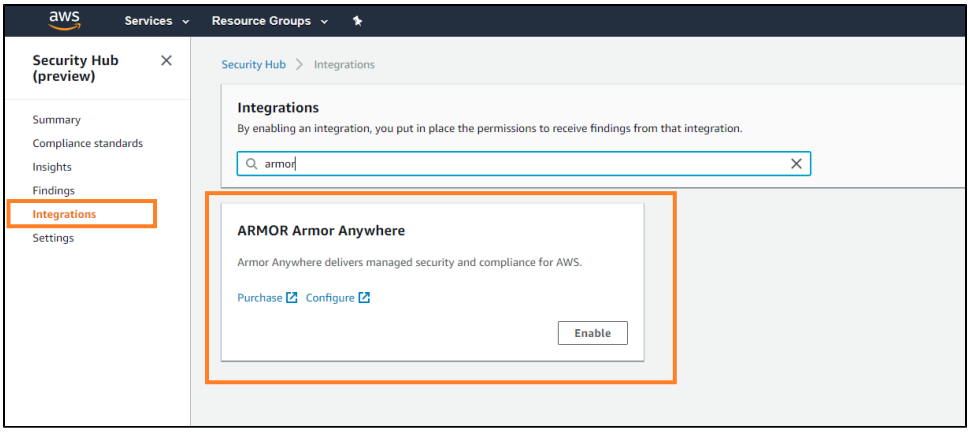


27. Return to the **Cloud Connections** screen in AMP.
28. Paste the **Role ARN** information into the **IAM Role ARN** field.
29. Click **Save Cloud Connection**.
    - Once the newly added cloud connections gathers data, the instance will appear in the **Virtual Machines** screen.

Step 2: Configure your AWS regions

In this step, you will enable AWS Security Hub in the desired AWS regions; this action will capture the findings from Security Hub in every configured region.

1. Access the AWS console.
2. Access the **Security Hub** section.
3. In the left-side navigation, click **Integrations**.
4. Locate and select **ARMOR Armor Anywhere**.



5. Click **Enable**.
6. In the pop-up window, click **Enable**.

Additional Documentation

To learn about the basics of Cloud Connections, see ANYWHERE Cloud Connections.

Was this helpful?

Your Rating: Results: 4 rates