IRON FORT

Granting IronFort Access to Your AWS Environment

What Is This?

IronFort is a compliance and security platform that scans your AWS environment to identify vulnerabilities, misconfigurations, and potential risks. This helps your organization stay secure and meet compliance requirements.

To perform these scans, IronFort uses an **AWS IAM User** — a dedicated account created specifically for IronFort's scanning service. You will be granting this user **read-only access** to your AWS account. This means IronFort can view your configuration and resources, but **cannot make any changes** to your environment.

How IronFort Accesses Your Account

- You create a dedicated IAM user in your AWS account for IronFort.
- You grant that user read-only permissions using AWS's built-in security policies.
- You provide IronFort with the user's access credentials (Access Key ID and Secret Access Key).
- When a scan runs, IronFort authenticates using these credentials and reads your AWS configuration — nothing is modified, deleted, or created.
- All data collected is handled in accordance with IronFort's privacy and security policies.

Step-by-Step Setup Instructions

What You Will Need

- Access to the AWS Management Console
- Administrative permissions to create IAM users and assign policies
- A secure method to share credentials with IronFort (your IronFort contact will provide guidance)

Step 1 — Sign In to AWS Console

1. Go to https://console.aws.amazon.com
2. Sign in with your AWS account credentials.

Step 2 — Navigate to IAM

1. In the AWS Console search bar at the top, type **IAM** and press Enter.
2. Click on **IAM** from the search results to open the Identity and Access Management console.

Step 3 — Create a New IAM User

1. In the left-hand menu, click **Users**.

2. Click the **Create user** button.
3. Enter a username such as `ironfort-scanner`.
4. Click **Next**.

Step 4 — Set Permissions

1. On the permissions page, select **Attach policies directly**.
2. In the search box, type `ReadOnlyAccess`.
3. Check the box next to **ReadOnlyAccess** (this is an AWS managed policy).

> ***Note:*** *The ReadOnlyAccess policy grants read-only permissions to all AWS services and resources. IronFort can view your configuration but cannot make any changes.*

4. Click **Next**.

Step 5 — Review and Create User

1. Review the user details and permissions.
2. Click **Create user**.

Step 6 — Enable Console Access (Optional but Recommended)

This allows IronFort compliance specialists to review your environment through the AWS Console if needed.

1. After creating the user, click on the username (`ironfort-scanner`) in the users list.
2. Click on the **Security credentials** tab.
3. Scroll down to **Console sign-in** section.
4. Click **Enable console access**.
5. Choose **Custom password** and create a strong password.
6. Uncheck **User must create a new password at next sign-in** (unless you prefer to rotate it).
7. Click **Apply**.
8. Save the console sign-in URL, username, and password securely.

Step 7 — Generate Access Keys

1. On the same **Security credentials** tab, scroll to **Access keys**.
2. Click **Create access key**.
3. Select **Third-party service** as the use case.
4. Check the confirmation box at the bottom.
5. Click **Next**.
6. Optionally, add a description tag like `IronFort scanner access`.
7. Click **Create access key**.

Step 8 — Save Your Credentials

Important: This is the only time you can view the Secret Access Key.

1. You will see:
    - **Access key ID** (e.g., `AKIAIOSFODNN7EXAMPLE`)
    - **Secret access key** (e.g., `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)

2. Click **Download .csv file** to save these credentials securely.

> ***Security Note:*** *Treat these credentials like passwords. Do not share them via email or unsecured channels. Your IronFort contact will provide you with a secure method to transmit these credentials.*

3. Click **Done**.

Step 9 — Share Credentials with IronFort

Contact your IronFort representative and provide them with:

- **Access Key ID**
- **Secret Access Key**
- **Console sign-in URL** (if console access was enabled)
- **Username and password** (if console access was enabled)

Use the secure credential-sharing method recommended by your IronFort contact.

Step 10 — Confirm Access

Once IronFort receives the credentials, they will verify the connection and begin your first scan. They will notify you when the setup is complete.

Frequently Asked Questions

Can IronFort make changes to my AWS environment? No. The ReadOnlyAccess policy is strictly read-only. IronFort cannot create, modify, or delete any AWS resources.

What data does IronFort collect? IronFort reads resource configurations (e.g., security groups, S3 bucket settings, IAM policies) to check for security and compliance issues. No application data or sensitive customer data is accessed.

Can I revoke access? Yes, at any time. Simply go to **IAM > Users**, select the `ironfort-scanner` user, and either delete the user or deactivate/delete the access keys.

How should I securely share the access keys? Never send access keys via regular email. Your IronFort contact will provide you with a secure sharing method, such as a password-protected document, encrypted email, or a secure credential-sharing platform.

Do I need to rotate these credentials? While not required, AWS recommends rotating access keys periodically for security best practices. If you rotate the keys, simply provide the new credentials to IronFort using a secure method.

What if I have multiple AWS accounts? If your organization uses multiple AWS accounts (e.g., production, staging, development), you will need to repeat these steps for each account you want IronFort to scan. Consider using AWS Organizations and role-based access for easier management across multiple accounts — contact IronFort for guidance.

Need Help?

If you have any questions or need assistance with these steps, please don't hesitate to reach out to us.

Email: hello@goironfort.com

We're happy to walk you through the setup or answer any questions you may have.