

**SecurITPosture**

Customer guide

# Connect AWS with an access key

The last resort. Not recommended for federal customers.

Version 0.1.0

Generated 2026-10-16

Draft: steps are specified but not final.

Vesta Cyber Solutions. Made from the same source as the guide on the web, so the two always match.

# Contents

|                          |   |
|--------------------------|---|
| Steps                    | 3 |
| The read policy          | 3 |
| How the key is protected | 4 |
| Rotate the key           | 4 |
| If it does not connect   | 4 |

**Not recommended for federal customers.**

Draft, pending the appliance build. This way to connect is built and tested in the product. The steps may change before release.

Use this way only when neither the instance role nor IAM Roles Anywhere is possible. A static access key is a long lived secret, and many federal environments do not allow one.

The appliance reads your account and never changes it.

## Steps

1. In IAM, create a dedicated user for SecurITPosture. Give it no console access. Never use the root user's key: the product refuses it.
2. Attach the read policy below to the user. If you will use a role in another account, give the user permission to assume that role instead, and attach the read policy to the role.
3. Create an access key for the user. AWS shows the secret once; keep it ready.
4. In SecurITPosture, open Integrations, then AWS, then Add AWS integration, and choose Access key. The product labels it "Not recommended for federal customers".
5. Enter the account name, the account ID, the access key ID (AKIA followed by 16 letters or digits), the secret access key (40 characters), the role ARN if you use one, the regions, and how often to scan.
6. Choose Add and validate. The product validates the connection before it marks the account connected. Without a role ARN, the key itself signs the reads, so the user needs the read policy directly.

## The read policy

This is the minimum the product needs to validate the account and discover its instances:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

The product adds what the evidence checks and the system's active Key Security Indicator checks read. The full list, and what each check reads, is on Connect AWS with the instance role. Always copy the policy from the product's setup page.

## How the key is protected

---

- The key ID and secret are stored together, encrypted with the appliance's field encryption key.
- After the request that saves it, the secret is never shown again. It is never written to a log, an export, an audit event, or the browser.
- With a role ARN, the appliance uses the key only to assume that role, for 15 minutes at a time.

## Rotate the key

---

1. When the key is older than 90 days, its card shows "Rotate this access key" and the system administrator gets a task. The 90 days count from when the product received the key.
2. Create a new access key for the same user in IAM. A user can hold two keys at once.
3. In SecurITPosture, choose Replace key on the account's card and enter the new key.
4. The product validates the new key first. The old key stays in use until the new one works.
5. In IAM, deactivate the old key, confirm the next run succeeds, then delete it.

Each rotation is recorded in the audit log without either key.

## If it does not connect

---

The product names the step that is missing, never a credential: for example the user's policy, or the role the user may assume.

To move off an access key once another way is possible, see [Change how an account connects](#).

See also [Instance role](#) and [IAM Roles Anywhere](#).