

SecurITPosture

Customer guide

Connect AWS with IAM Roles Anywhere

The way to connect when the appliance runs outside AWS, using a certificate.

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

Choose the certificate	3
Steps	3
The read policy	4
If it does not connect	4
Renewing the certificate	4
What is stored	5

Draft, pending the appliance build. This way to connect is built and tested in the product; its proof against a live AWS account is still to come, and the steps may change before release.

Use this way when the appliance runs outside AWS, for example on VMware, Hyper-V, or Azure. The appliance proves who it is with a certificate and receives temporary AWS credentials, renewed before they expire. No long lived key is stored.

As of October 2026, AWS lists IAM Roles Anywhere as in scope for FedRAMP: Moderate in the commercial East and West regions and High in AWS GovCloud (US). Check the AWS FedRAMP services in scope page for the current status.

The appliance reads your account and never changes it.

Choose the certificate

When you add the account, choose one of two certificates:

- **This server's certificate.** The product issues it from your workspace's own certificate authority (CA), which it creates the first time anyone needs it. Each workspace has its own CA, so no other workspace's certificate is ever trusted by your AWS account. The certificate is valid for one year and is renewed for you (see below). Nothing to upload.
- **Your own certificate.** An end entity certificate from your organization's CA, with its private key, and any intermediate CA certificates (up to four). It must be an end entity certificate (not a CA), allow digital signatures, allow client authentication if it lists extended key uses, match its key, be valid today, and use an ECDSA P-256 key or an RSA key of 2048 to 4096 bits.

Either way the private key is stored encrypted inside the appliance and is never shown again.

Steps

The add dialog shows these steps before it asks for anything, because the trust anchor in AWS comes first.

1. In SecurITPosture, open Integrations, then AWS, then Add AWS integration, and choose Certificate (IAM Roles Anywhere). Only a system administrator or a compliance analyst can add an integration.
2. Choose the certificate. For this server's certificate, choose Download this workspace's CA certificate in the dialog. For your own, use your CA certificate.
3. In the AWS console, open IAM Roles Anywhere and create a trust anchor. Choose External certificate bundle and paste the CA certificate.
4. Create a read only IAM role with the trust policy the dialog shows. It allows only the service `rolesanywhere.amazonaws.com`, only the certificate's subject (its common name), and only through your trust anchor. Replace the placeholder with your trust anchor's ARN; for your own certificate, also put in your certificate's common name. For this server's certificate the common name is `securitposture-` followed by the account ID.
5. Create a profile in IAM Roles Anywhere that lists the role.

6. Back in the dialog, enter the account name, the account ID, the trust anchor ARN, the profile ARN, the role ARN, the regions, and how often to scan. The trust anchor and the profile must be in the account you connect and in one region.
7. Choose Add and validate. The product connects, checks that the account answering is the one you entered, and checks every region before it marks the account connected. It then shows the read policy to attach to the role.

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 setup page shows the full policy to attach, which adds what the evidence checks and the system's Key Security Indicator checks read. The permissions are the same in every way of connecting; 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, or choose Policies on the account's card while it is not connected.

If it does not connect

The product names the step to fix, never a credential:

- "The trust anchor or the profile was not found": check both ARNs, and that both are in the same region.
- "AWS refused the certificate": check that the trust anchor was made from the right CA certificate, that the profile lists the role, and that the role's trust policy names `rolesanywhere.amazonaws.com` and this certificate's subject.
- "The certificate cannot be used", with the reason: the uploaded certificate failed one of the checks above.
- A missing permission: attach the read policy to the role the profile lists.

Renewing the certificate

- **This server's certificate** is renewed from your workspace's CA on the next run once it is within 30 days of expiry, or at once when you choose Validate on the account's card. The new certificate is checked against AWS before it replaces the old one; until then the old one stays in use. If a renewal keeps failing within 7 days of expiry, the card says "This server's certificate could not be

renewed" with the date, and the analyst gets a task.

- **Your own certificate** shows "Renew this certificate" on the card within 30 days of expiry, and the system administrator gets a task. Issue a new certificate from your CA, then choose Replace certificate on the card and paste the new certificate, its key, and any intermediates. The product checks the new certificate against AWS first; until it validates, the old one stays in use.

Each renewal and replacement is recorded in the audit log by certificate serial number, never with a key.

What is stored

The account ID, the three ARNs, the certificate's serial number and expiry, whether it is your own, the regions, and the scan frequency. The certificate, its private key, and any chain are stored encrypted with the appliance's field encryption key; your workspace's CA key is stored the same way. No Vesta credentials are stored. Error logs hold AWS error codes and request IDs only. The appliance's outbound firewall allows the AWS endpoints only while an AWS integration is connected.

See also Instance role, Access key, and Change how an account connects.