PROWLER

Maximize your Cloud Security Compliance Assessments

with Open Source and a pinch of AI

Andoni & Pedro ~ cfgmgmtcamp 2026

$ aws sts get-caller-identity

Security & Compliance Engineer at Prowler

/pedro-martin-gon

pedrooot

Cloud Security Engineer at Prowler

/andoniaf

andoniaf

Agenda

CLI
Command Line Interface

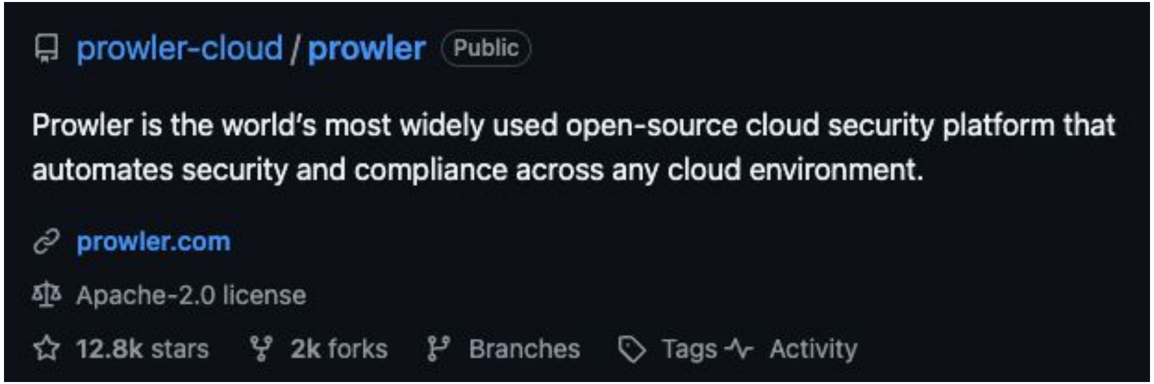
APP/Cloud
Full tour thru our amazing project

MCP
Of course! AI time

Contributing
Do you want to improve things?

Great ideas? Go for it!

What is Prowler?



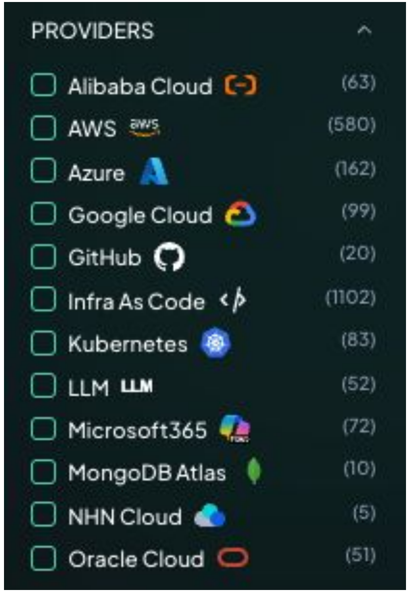
prowler-cloud / prowler Public

Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment.

prowler.com

Apache-2.0 license

12.8k stars 2k forks Branches Tags Activity



PROVIDERS

☐ Alibaba Cloud	(63)
☐ AWS	(580)
☐ Azure	(162)
☐ Google Cloud	(99)
☐ GitHub	(20)
☐ Infra As Code	(1102)
☐ Kubernetes	(83)
☐ LLM	(52)
☐ Microsoft365	(72)
☐ MongoDB Atlas	(10)
☐ NHN Cloud	(5)
☐ Oracle Cloud	(51)

Prowler is the world's most widely used open-source (ALv2) tool for cloud security

40M+
downloads

1M+
downloads/week

300+
contributors

What is Prowler? Product and Services: Our Platform

Prowler Project (CLI and self-hosted app)

- Open Source Multi-Cloud Security Scanner for AWS, Azure, GCP, K8s, Github and more
- Continuous monitoring, security assessments and audits, incident response, compliance, hardening and forensics readiness.
- Runs on-premises and in the cloud.
- Includes CLI, SDK, API, and UI for versatility.
- github.com/prowler-cloud/prowler

Prowler Cloud

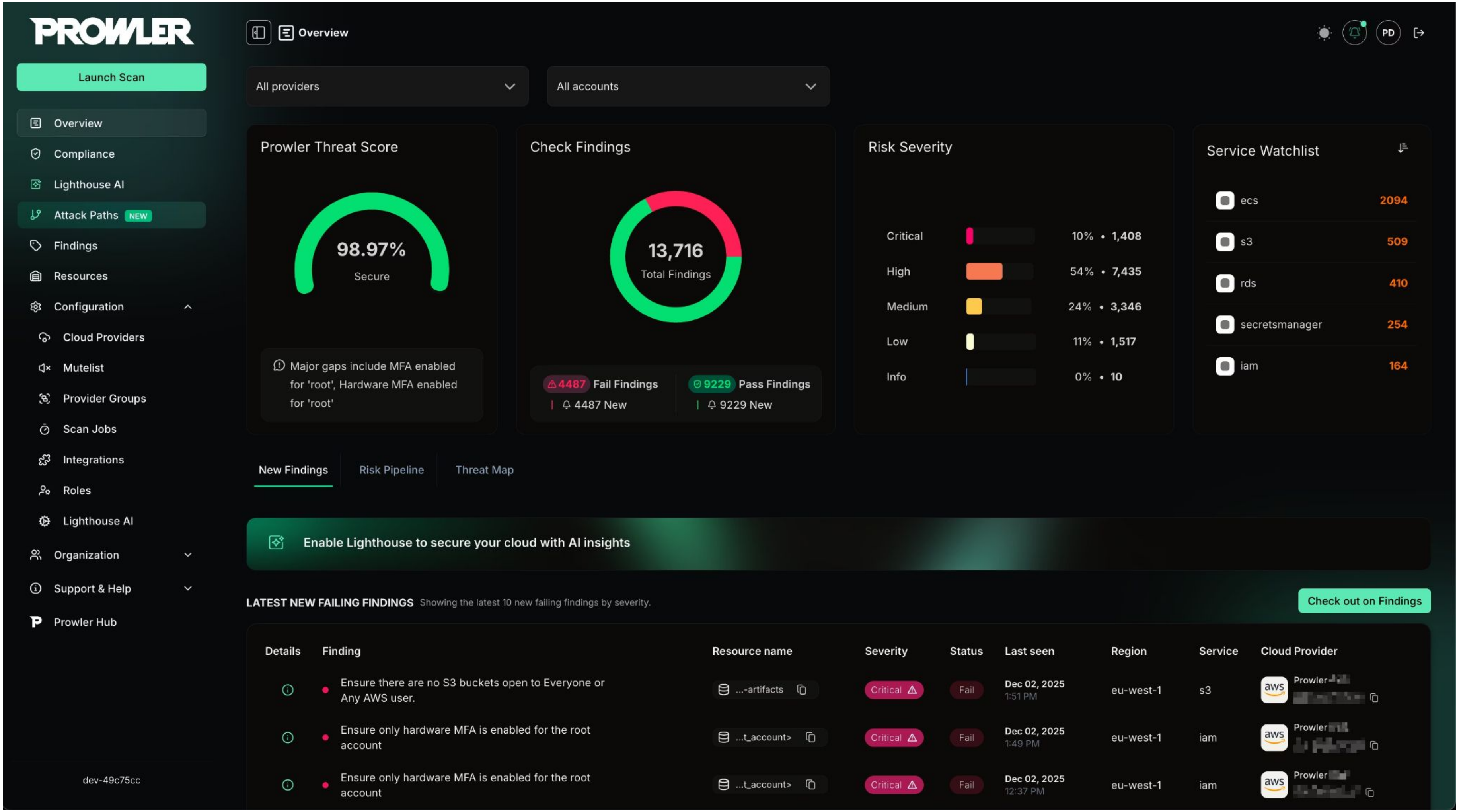
- Prowler Managed Service handles hosted Prowler with customer signups, billing, and management. Supports payments via Marketplaces and Stripe.
- Resource and Scan based pricing.
- 24x7 proactive monitoring by ProwlerPro, Inc
- Automatic updates, patching, and new versions with Backup and High-Availability setup
- Enterprise grade compliance (SOC2 Type 2)
- Enterprise Support SLA and more!
- cloud.prowler.com

Prowler Hub

- Public knowledge base with our artifacts covering providers, services, checks, remediations, code and more.
- All artifacts are exposed via API and web UI for easy consumption and two ways integration with Prowler, Prowler Studio and third parties.
- hub.prowler.com

Prowler Studio - MCP

- Create, share, and run detection checks, remediations, and compliance frameworks using our online SDK and AI.
- https://github.com/prowler-cloud/prowler-studio



Prowler Threat Score

98.97%
Secure

Major gaps include MFA enabled for 'root', Hardware MFA enabled for 'root'

Check Findings

13,716
Total Findings

4487 Fail Findings | 4487 New

9229 Pass Findings | 9229 New

Risk Severity

Critical	10%	1,408
High	54%	7,435
Medium	24%	3,346
Low	11%	1,517
Info	0%	10

Service Watchlist

ecs	2094
s3	509
rds	410
secretsmanager	254
iam	164

Enable Lighthouse to secure your cloud with AI insights

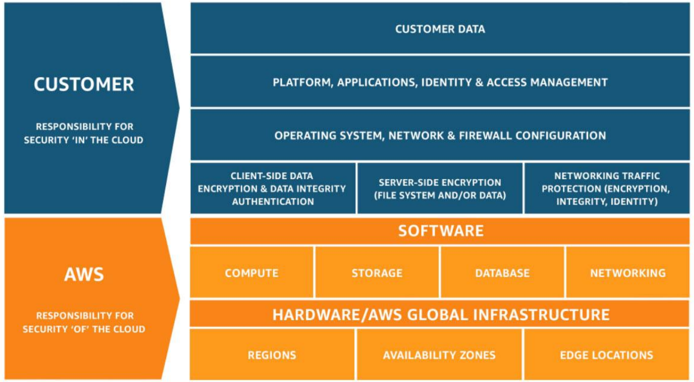
LATEST NEW FAILING FINDINGS Showing the latest 10 new failing findings by severity.

Details	Finding	Resource name	Severity	Status	Last seen	Region	Service	Cloud Provider
ⓘ	● Ensure there are no S3 buckets open to Everyone or Any AWS user.	...-artifacts	Critical ⚠	Fail	Dec 02, 2025 1:51 PM	eu-west-1	s3	aws Prowler [redacted]
ⓘ	● Ensure only hardware MFA is enabled for the root account	...t_account>	Critical ⚠	Fail	Dec 02, 2025 1:49 PM	eu-west-1	iam	aws Prowler [redacted]
ⓘ	● Ensure only hardware MFA is enabled for the root account	...t_account>	Critical ⚠	Fail	Dec 02, 2025 12:37 PM	eu-west-1	iam	aws Prowler [redacted]

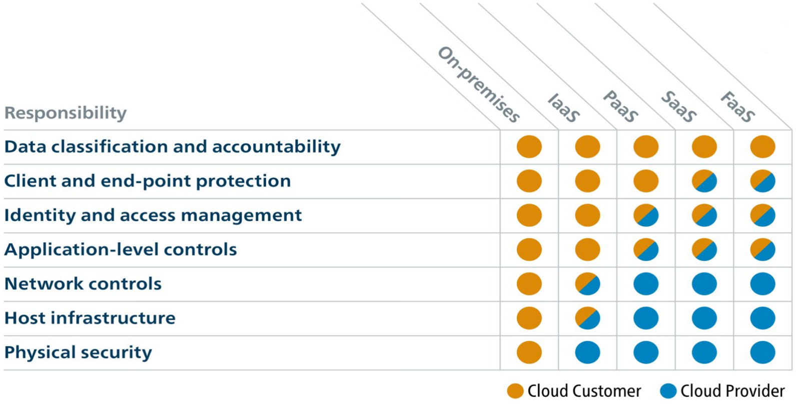
And why do I need Prowler?

Top 5 Cloud Security Threats & Common Attacks

1. **Misconfigurations**
   - Public exposed resources, weak IAM policies, unrestricted security groups
2. **IAM vulnerabilities**
   - Credential theft, privilege escalation, brute force attacks
3. **Insecure APIs and Interfaces**
   - API key leaks, MITM attacks, rate-limiting bypass
4. **Data Breaches and Exfiltration**
   - Unencrypted data exposure, insider threats, SQL injection attacks.
5. **Inadequate Monitoring and Logging**
   - Log tampering, cryptojacking, lack of real-time alerts


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

From https://aws.amazon.com/es/compliance/shared-responsibility-model/

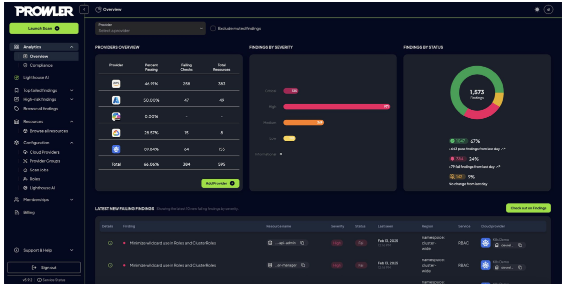


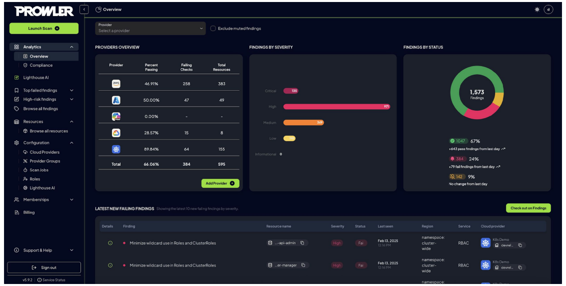
Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	🟠	🟠	🟠	🟠	🟠
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Network controls	🟠	🟠🔵	🔵	🔵	🔵
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵
Physical security	🟠	🔵	🔵	🔵	🔵

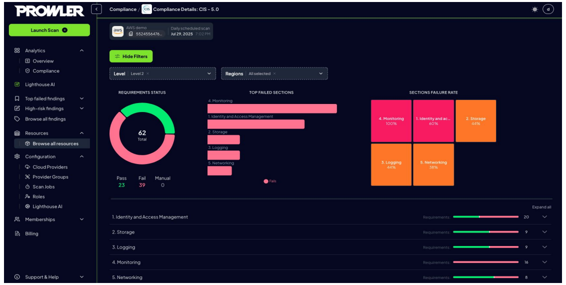
🟠 Cloud Customer 🔵 Cloud Provider

From https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

Prowler Use-Cases







Security Monitoring

Address security risks before they become incidents

- Minimize financial impact of theft, fraud, & remediation costs
- Protect sensitive data & IP
- Maintain customer trust & brand value

IaC monitoring

Static code analysis for Infrastructure as Code (Terraform, Cloudformation, Kubernetes YAML)

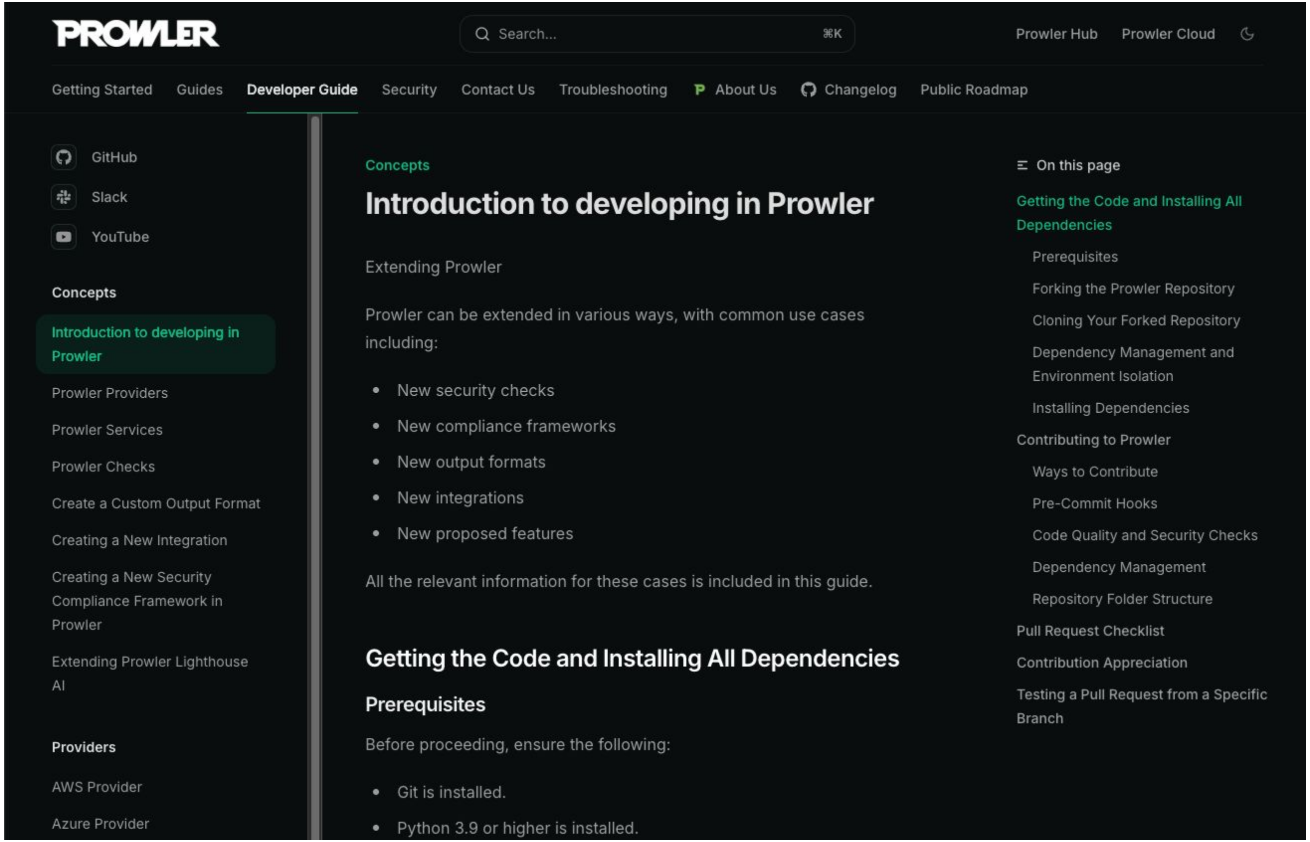
- Early detection of security risks
- Lifecycle coverage and DevOps integration of security posture
- Increased development velocity

Compliance

Audit & Compliance Assessments (including CIS, SOC2, HIPAA, PCI, CISA, NIST, ISO27001, etc.)

- Reduce audit burden
- Enable business growth & time-to-market
- Improve operational efficiency and cost-effectiveness

How to contribute?



Concepts

- Introduction to developing in Prowler
- Prowler Providers
- Prowler Services
- Prowler Checks
- Create a Custom Output Format
- Creating a New Integration
- Creating a New Security Compliance Framework in Prowler
- Extending Prowler Lighthouse AI

Providers

- AWS Provider
- Azure Provider

Concepts

Introduction to developing in Prowler

Extending Prowler

Prowler can be extended in various ways, with common use cases including:

- New security checks
- New compliance frameworks
- New output formats
- New integrations
- New proposed features

All the relevant information for these cases is included in this guide.

Getting the Code and Installing All Dependencies

Prerequisites

Before proceeding, ensure the following:

- Git is installed.
- Python 3.9 or higher is installed.

On this page

- Getting the Code and Installing All Dependencies
  - Prerequisites
  - Forking the Prowler Repository
  - Cloning Your Forked Repository
  - Dependency Management and Environment Isolation
  - Installing Dependencies
- Contributing to Prowler
  - Ways to Contribute
  - Pre-Commit Hooks
  - Code Quality and Security Checks
  - Dependency Management
  - Repository Folder Structure
- Pull Request Checklist
- Contribution Appreciation
- Testing a Pull Request from a Specific Branch

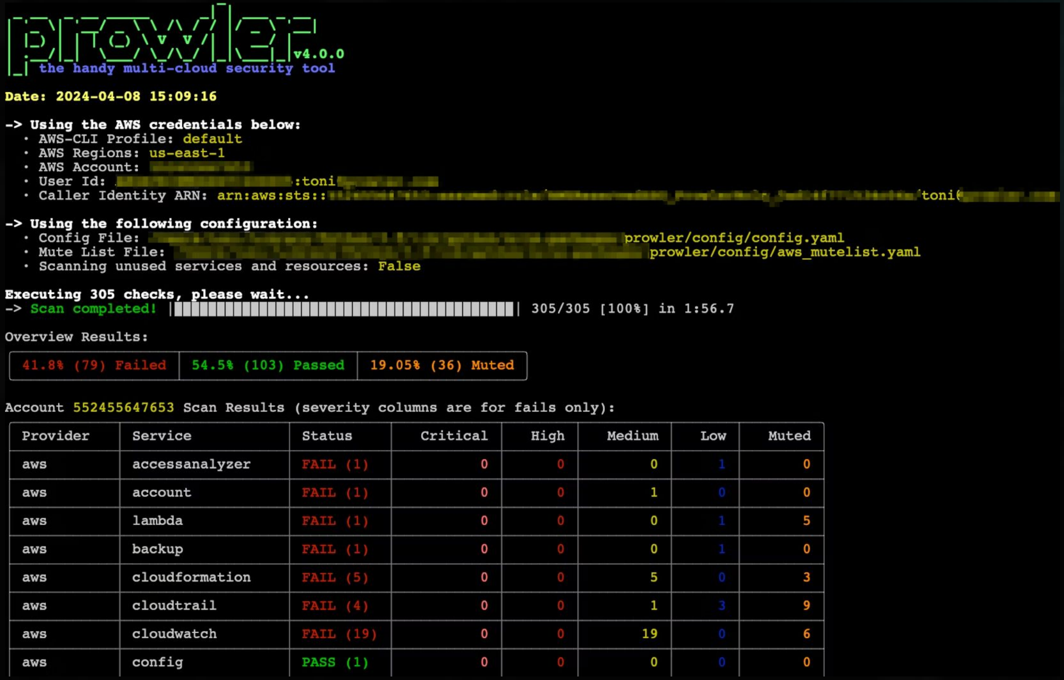
goto.prowler.com/devguide

roadmap.prowler.com/roadmap

CLI

Prowler User

- Installation
- Scan
- Mutelisting
- Compliance
- Custom Checks
- Fixers



```
                                                    v4.0.0
    the handy multi-cloud security tool

Date: 2024-04-08 15:09:16

-> Using the AWS credentials below:
  · AWS-CLI Profile: default
  · AWS Regions: us-east-1
  · AWS Account: [redacted]
  · User Id: [redacted]:toni[redacted]
  · Caller Identity ARN: arn:aws:sts::[redacted]toni[redacted]

-> Using the following configuration:
  · Config File: [redacted]prowler/config/config.yaml
  · Mute List File: [redacted]prowler/config/aws_mutelist.yaml
  · Scanning unused services and resources: False

Executing 305 checks, please wait...
-> Scan completed! |████████████████████████████████████████| 305/305 [100%] in 1:56.7

Overview Results:
╭─────────────────────┬──────────────────────┬─────────────────────╮
│ 41.8% (79) Failed   │ 54.5% (103) Passed   │ 19.05% (36) Muted   │
╰─────────────────────┴──────────────────────┴─────────────────────╯

Account 552455647653 Scan Results (severity columns are for fails only):
╭────────────┬────────────────────┬────────────┬────────────┬────────┬──────────┬───────┬─────────╮
│ Provider   │ Service            │ Status     │   Critical │   High │   Medium │   Low │   Muted │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ accessanalyzer     │ FAIL (1)   │          0 │      0 │        0 │     1 │       0 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ account            │ FAIL (1)   │          0 │      0 │        1 │     0 │       0 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ lambda             │ FAIL (1)   │          0 │      0 │        0 │     1 │       5 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ backup             │ FAIL (1)   │          0 │      0 │        0 │     1 │       0 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ cloudformation     │ FAIL (5)   │          0 │      0 │        5 │     0 │       3 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ cloudtrail         │ FAIL (4)   │          0 │      0 │        1 │     3 │       9 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ cloudwatch         │ FAIL (19)  │          0 │      0 │       19 │     0 │       6 │
├────────────┼────────────────────┼────────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ config             │ PASS (1)   │          0 │      0 │        0 │     0 │       0 │
```

PROWLER

CLI

Lab 0 - Installation

Inside your environment shell, run the following commands to make sure Prowler v5 and Python are ready:

```
python3 --version # >=3.9, <=3.12
pipx install prowler #  https://pipx.pypa.io/stable/installation/
prowler -v
```

To make sure you have the latest version do:

```
pipx upgrade prowler
```

CLI

Lab 1: AWS Authentication in Prowler

Make sure you have properly configured your AWS-CLI with a valid Access Key and Region or declare AWS variables properly (or instance profile/role):

```
aws configure
```

or

```
export AWS_ACCESS_KEY_ID="ASXXXXXXX"
export AWS_SECRET_ACCESS_KEY="XXXXXXXXX"
export AWS_SESSION_TOKEN="XXXXXXXXX"
```

To use a particular AWS profile (~/.aws/credentials or ~/.aws/config)

```
prowler aws -p <profile_name>
```

Permissions templates: https://github.com/prowler-cloud/prowler/tree/master/permissions

```
arn:aws:iam::aws:policy/SecurityAudit
arn:aws:iam::aws:policy/job-function/ViewOnlyAccess
```

https://tinyurl.com/bddxch2n

CLI

Lab 1: AWS Role Assumption

Set-up custom profile in: `~/.aws/config` with all the needed information. Then, use

```
prowler aws -p/--profile your-custom-profile
```

Profile example:

```
[profile crossaccountrole]
role_arn = arn:aws:iam::234567890123:role/SomeRole
credential_source = EcsContainer
```

Prowler can assume an IAM role in remote or the same account to scan.

In Prowler v5, parameters are merged in a single flag → -R/--role <role_arn>

```
prowler aws -R arn:aws:iam::123456789012:role/ProwlerRole
```

Optional flags when assuming a role:

- -T/--session-duration <seconds> *by default 3600 seconds
- -I/--external-id <external_id>

CLI

Lab 2: GitHub

Automatic Login Method Detection

If no login method is explicitly provided, Prowler will automatically attempt to authenticate using environment variables in the following order of precedence:

```
GITHUB_PERSONAL_ACCESS_TOKEN
GITHUB_OAUTH_APP_TOKEN
GITHUB_APP_ID and GITHUB_APP_KEY (where the key is the content of the
private key file)
```

- Personal Access Token (PAT) -> `prowler github --personal-access-token pat`
- OAuth App Token -> `prowler github --oauth-app-token oauth_token`
- GitHub App Credentials -> `prowler github --github-app-id app_id --github-app-key-path app_key_path`

Quick Test:

```
export GITHUB_PERSONAL_ACCESS_TOKEN=$(gh auth token)
prowler github
```

CLI

Lab 3: IaC

Prowler CLI supports the following scanners:

- Vulnerability
- Misconfiguration
- Secret
- License

By default, only misconfiguration and secret scanners run during a scan.

- Scan directory -> `prowler iac --scan-path ./my-iac-directory`
- Remote GH repository -> `prowler iac --scan-repository-url https://github.com/user/repo.git`
- Specify Scanners -> `prowler iac --scan-path ./my-iac-directory --scanners vuln misconfig`

CLI

Lab 4: Mutelisting

The *Mutelist* feature can be used to “skip” PASS or FAIL findings that sometimes are either not important or an assumed risk. For example, an AWS S3 bucket open to the internet hosting a web site.

```
Mutelist:
  Accounts:
    "123456789012":
      Checks:
        "iam_user_hardware_mfa_enabled":
          Regions:
            - "us-east-1"
          Resources:
            - "user-1"           # Will mute user-1 in check iam_user_hardware_mfa_enabled
            - "user-2"           # Will mute user-2 in check iam_user_hardware_mfa_enabled
        "ec2_*":
          Regions:
            - "*"
          Resources:
            - "*"                 # Will mute every EC2 check in every account and region
        "*":
          Regions:
            - "*"
          Resources:
            - "test"
          Tags:
            - "test=test"         # Will mute every resource containing the string "test" and the tags 'test=test' and
            - "project=test|project=stage" # either of ('project=test' OR project=stage) in account 123456789012 and every
region
```

PROWLER

CLI

Lab 5: Compliance

- Prowler supports Compliance Frameworks for AWS, Azure, GCP, K8S ...(e.g., CIS, PCI-DSS, etc.)

- Each Compliance Framework:
  - Has different requirements that match with one or more Prowler checks.
  - Will create a dedicated report based on its own requirements and the result of the scan in CSV.

- Definition JSON per Compliance Framework with all the information and the mapping of the checks are located in `prowler/compliance/<provider>/`

- Run the checks of a specific compliance framework from a provider with:

```
prowler <provider> --compliance <compliance>
```

  - *E.g.:* `.prowler aws --compliance cis_1.5_aws`

CLI

Lab 5: Compliance II

```
{
        "Framework": "<framework>",
        "Version": "<version>",
        "Provider": "<provider>",
        "Description": "Compliance Framework full description",
        "Requirements": [
                {
                "Id": "<unique-id>",
                "Name": "Requirement Name",
                "Description": "Requirements full description",
                "Checks": [
                        "Here is the prowler check or checks that is going to be executed"
                ],
                "Attributes": [
                        {
                                <Custom attributes for the Requirement>
                        }
                ]
                },
                ...
        ]
}
```

PROWLER

CLI

Lab 5: Compliance III

- List all available compliance frameworks of a provider with:

```
prowler <provider> --list-compliance
```

  - *E.g.:* `prowler aws --list-compliance`

- List compliance requirements for a given compliance with:

```
prowler <provider> --list-compliance-requirements <compliance>
```

  - *E.g.:* `prowler aws --list-compliance-requirements cis_1.5_aws`

- Run the checks of a specific compliance framework from a provider with:

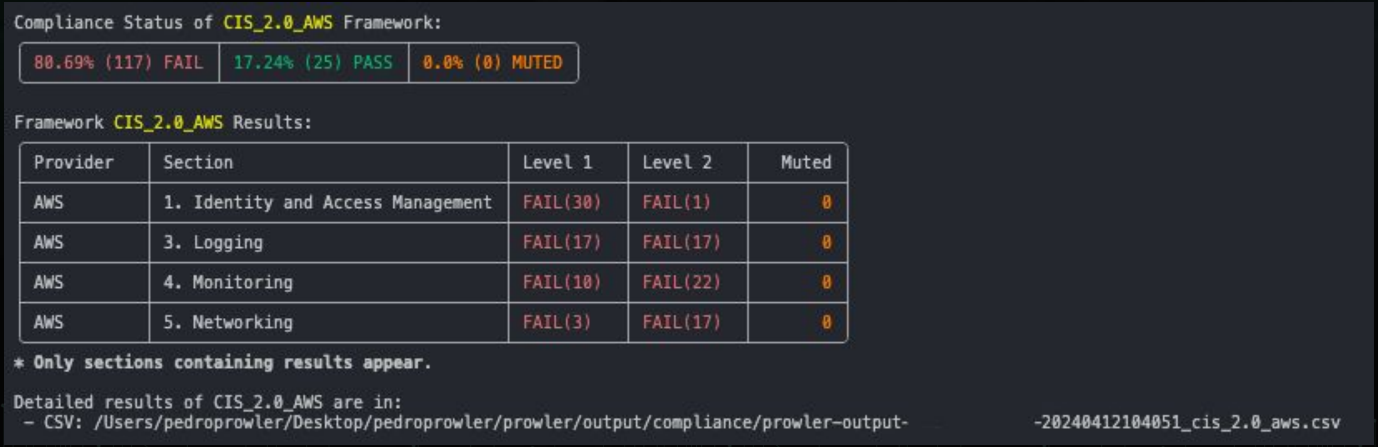
```
prowler <provider> --compliance <compliance>
```

  - *E.g.:* `prowler aws --compliance cis_1.5_aws`

CLI

Lab 5: Compliance IV

1. List the available compliance frameworks
    - ○ `prowler <provider> --list-compliance`
2. Choose one compliance framework and run Prowler based on that compliance:
    - ○ `E.g: prowler aws --compliance cis_2.0_aws`

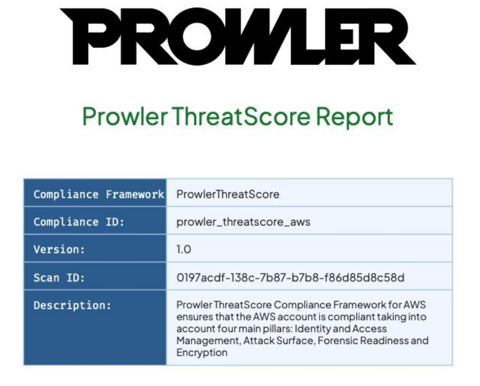


```
Compliance Status of CIS_2.0_AWS Framework:
┌──────────────────┬─────────────────┬──────────────────┐
│ 80.69% (117) FAIL │ 17.24% (25) PASS │ 0.0% (0) MUTED │
└──────────────────┴─────────────────┴──────────────────┘

Framework CIS_2.0_AWS Results:
┌──────────┬─────────────────────────────────┬──────────┬──────────┬─────────┐
│ Provider │ Section                         │ Level 1  │ Level 2  │   Muted │
├──────────┼─────────────────────────────────┼──────────┼──────────┼─────────┤
│ AWS      │ 1. Identity and Access Management │ FAIL(30) │ FAIL(1)  │       0 │
├──────────┼─────────────────────────────────┼──────────┼──────────┼─────────┤
│ AWS      │ 3. Logging                      │ FAIL(17) │ FAIL(17) │       0 │
├──────────┼─────────────────────────────────┼──────────┼──────────┼─────────┤
│ AWS      │ 4. Monitoring                   │ FAIL(10) │ FAIL(22) │       0 │
├──────────┼─────────────────────────────────┼──────────┼──────────┼─────────┤
│ AWS      │ 5. Networking                   │ FAIL(3)  │ FAIL(17) │       0 │
└──────────┴─────────────────────────────────┴──────────┴──────────┴─────────┘
* Only sections containing results appear.

Detailed results of CIS_2.0_AWS are in:
 - CSV: /Users/pedroprowler/Desktop/pedroprowler/prowler/output/compliance/prowler-output-          -20240412104051_cis_2.0_aws.csv
```

CLI

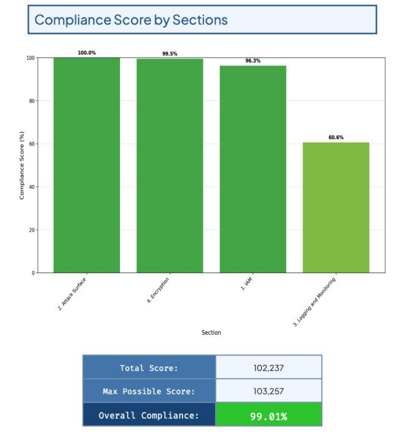
Lab 6: ThreatScore

Prowler ThreatScore identifies and highlights the most critical findings, giving each requirement a weighted score based on its severity. This allows you to quickly understand the level of risk, prioritize remediation, and focus on what needs fixing as soon as possible, all from a compliance-driven perspective, ready for a wrap-up or PDF report.



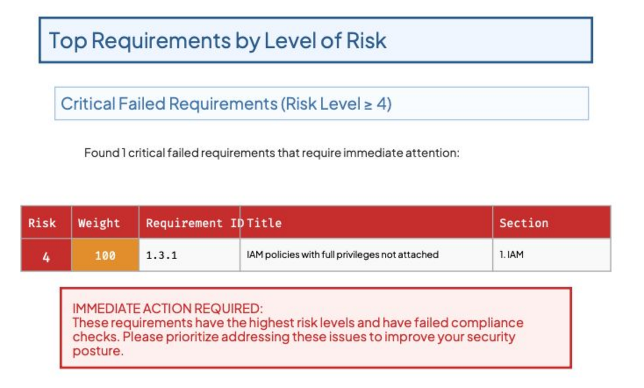
Prowler ThreatScore Report

Compliance Framework	ProwlerThreatScore
Compliance ID:	prowler_threatscore_aws
Version:	1.0
Scan ID:	0197acdf-138c-7b87-b7b8-f86d85d8c58d
Description:	Prowler ThreatScore Compliance Framework for AWS ensures that the AWS account is compliant taking into account four main pillars: Identity and Access Management, Attack Surface, Forensic Readiness and Encryption



Compliance Score by Sections

Total Score:	102,237
Max Possible Score:	103,257
Overall Compliance:	99.01%



Top Requirements by Level of Risk

Critical Failed Requirements (Risk Level ≥ 4)

Found 1 critical failed requirements that require immediate attention:

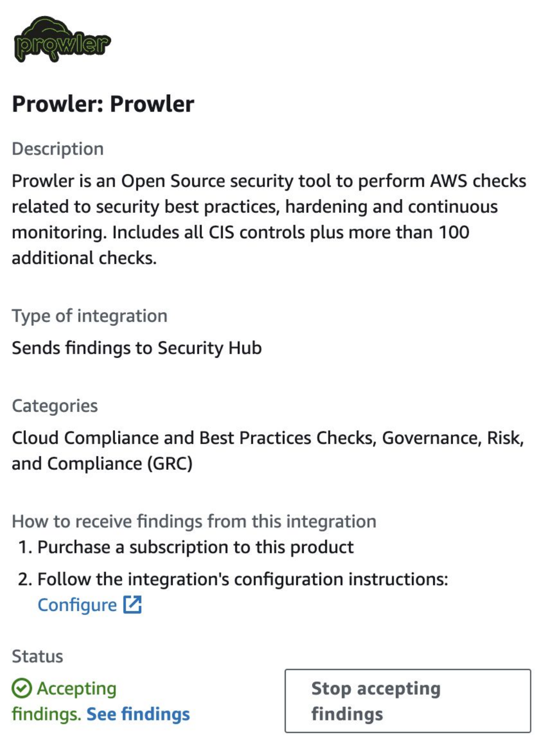
Risk	Weight	Requirement ID	Title	Section
4	100	1.3.1	IAM policies with full privileges not attached	1. IAM

IMMEDIATE ACTION REQUIRED:
These requirements have the highest risk levels and have failed compliance checks. Please prioritize addressing these issues to improve your security posture.

CLI

Lab 7: AWS Security Hub integration

- Prowler creates a JSON formatted as AWS Security Finding Format (ASFF) per finding.
- Sends each ASFF finding per region to Security Hub using the official integration.
- An entire list of ASFF findings is generated and store in an output json file.
- Using flag `-S` or `--security-hub`
- Adding flag `--status FAIL` will send only fails which will reduce the number of findings sent to Security Hub.
- Since Security Hub is region based, use `--region <region>`



Prowler: Prowler

Description

Prowler is an Open Source security tool to perform AWS checks related to security best practices, hardening and continuous monitoring. Includes all CIS controls plus more than 100 additional checks.

Type of integration

Sends findings to Security Hub

Categories

Cloud Compliance and Best Practices Checks, Governance, Risk, and Compliance (GRC)

How to receive findings from this integration

1. Purchase a subscription to this product
2. Follow the integration's configuration instructions: Configure

Status

✓ Accepting findings. See findings

CLI

Lab 8: Upload reports to a S3 Bucket

Use `prowler aws -B my-bucket`

If you can use a custom folder and/or filename, use `-o/--output-directory` and/or `-F/--output-filename`

```
prowler aws \
        -B my-bucket \
        --output-directory test-folder \
        --output-filename output-filename
```

By default Prowler sends HTML, JSON and CSV output formats, if you want to send a custom output format or a single one of the defaults you can specify it with the `-M/--output-modes` flag.

```
prowler aws -M csv -B my-bucket
```

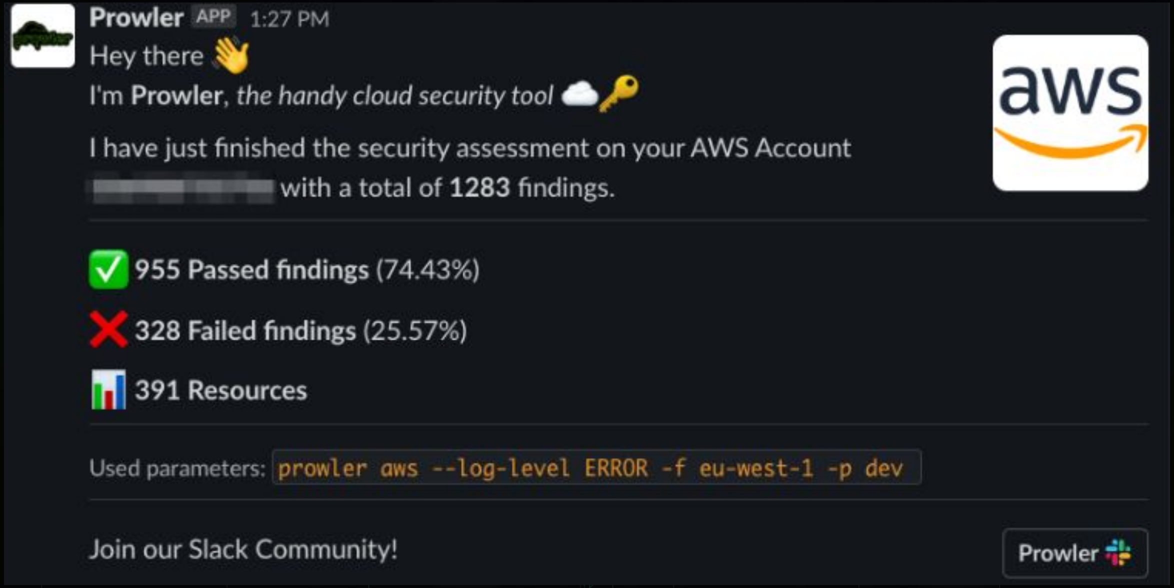
* Make sure that the used credentials have *s3:PutObject* permissions in the S3 path where the reports are going to be uploaded.

CLI

Lab 9: Slack Integration

Prowler can be integrated with Slack to send a summary of the execution having configured a Slack APP in your channel with the following command:

```
prowler <provider> --slack
```



Prowler APP 1:27 PM

Hey there 👋

I'm **Prowler**, *the handy cloud security tool* ☁️🔑

I have just finished the security assessment on your AWS Account [redacted] with a total of **1283** findings.

✅ **955 Passed findings** (74.43%)

❌ **328 Failed findings** (25.57%)

📊 **391 Resources**

Used parameters: `prowler aws --log-level ERROR -f eu-west-1 -p dev`

Join our Slack Community!

CLI

Lab 10: Custom Check Metadata

The custom metadata option offers a means to override default metadata set by Prowler

Use `--custom-checks-metadata-file`

- Severity
- CheckTitle
- Risk
- RelatedUrl
- Remediation
- Code
  - CLI
  - NativeIaC
  - Other
  - Terraform
- Recommendation
  - Text
  - Url

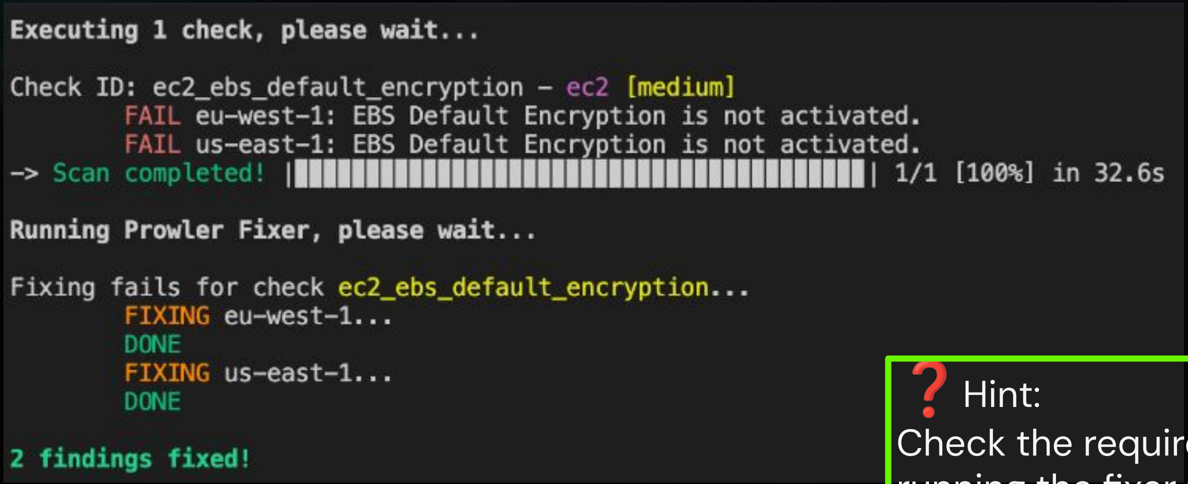
CLI

Lab 11: Fixers

Prowler allows you to fix some of the failed findings it identifies at scanning time.
Use `--list-fixer` to see all the available fixes for each provider.

Use `--fixer`:

```
prowler <provider> -c <check_to_fix_1> <check_to_fix_2> ... --fixer
```



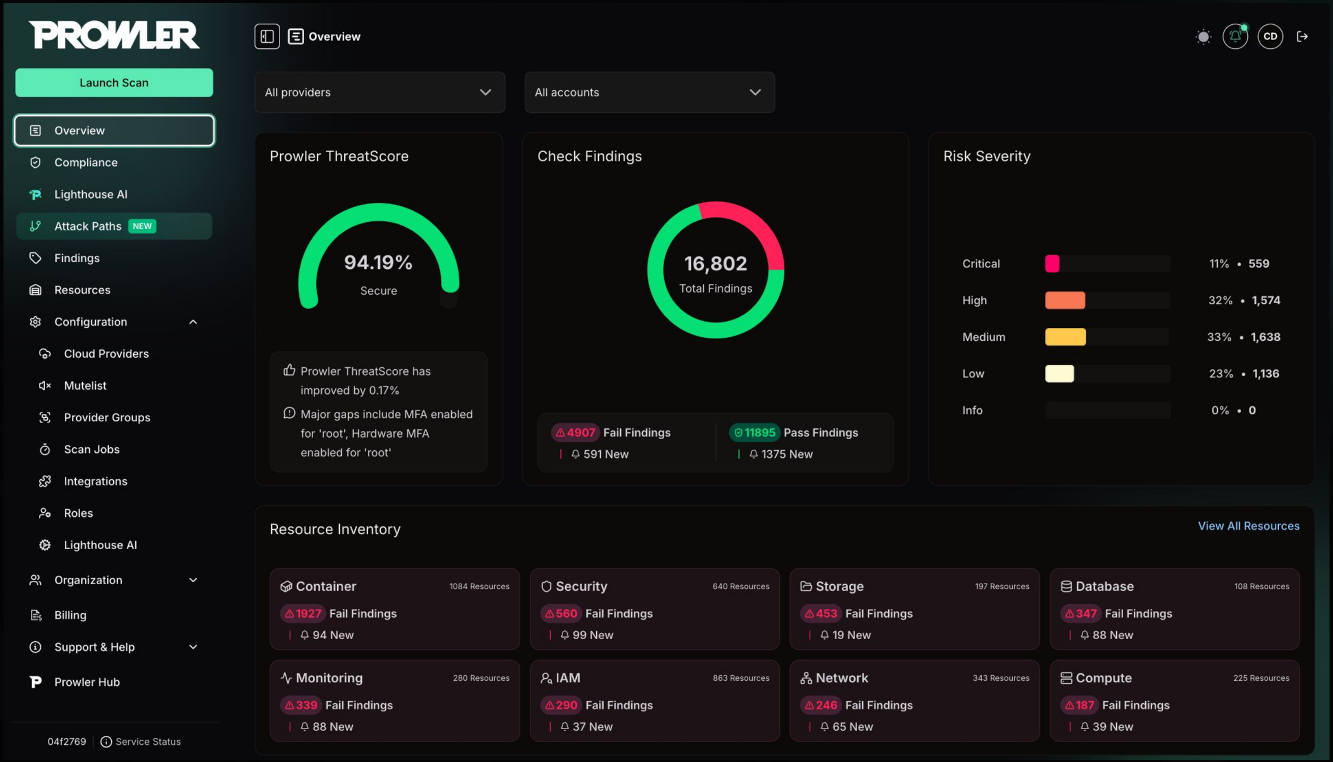
```
Executing 1 check, please wait...

Check ID: ec2_ebs_default_encryption - ec2 [medium]
        FAIL eu-west-1: EBS Default Encryption is not activated.
        FAIL us-east-1: EBS Default Encryption is not activated.
-> Scan completed! |████████████████████████████████████████| 1/1 [100%] in 32.6s

Running Prowler Fixer, please wait...

Fixing fails for check ec2_ebs_default_encryption...
        FIXING eu-west-1...
        DONE
        FIXING us-east-1...
        DONE

2 findings fixed!
```

❓ Hint:
Check the required permissions inside fixer file before running the fixer to ensure it can be executed.

APP

Prowler User

- Installation
- Add a Provider
- Run a Scan
- Check Findings
- Check Compliance
- Lighthouse AI 🤖
- RBAC
- Attack Paths



Prowler ThreatScore

94.19%
Secure

Prowler ThreatScore has improved by 0.17%

Major gaps include MFA enabled for 'root', Hardware MFA enabled for 'root'

Check Findings

16,802
Total Findings

4907 Fail Findings | 591 New

11895 Pass Findings | 1375 New

Risk Severity

Critical	11% • 559
High	32% • 1,574
Medium	33% • 1,638
Low	23% • 1,136
Info	0% • 0

Resource Inventory

Category	Resources	Fail Findings	New
Container	1084 Resources	1927 Fail Findings	94 New
Security	640 Resources	560 Fail Findings	99 New
Storage	197 Resources	453 Fail Findings	19 New
Database	108 Resources	347 Fail Findings	88 New
Monitoring	280 Resources	339 Fail Findings	88 New
IAM	863 Resources	290 Fail Findings	37 New
Network	343 Resources	246 Fail Findings	65 New
Compute	225 Resources	187 Fail Findings	39 New

App

Lab 12 - Installation

You can install the new Prowler App using Docker Compose:

```
curl -LO https://raw.githubusercontent.com/prowler-cloud/prowler/refs/heads/master/docker-compose.yml
curl -LO https://raw.githubusercontent.com/prowler-cloud/prowler/refs/heads/master/.env
docker compose up -d
```

Enjoy Prowler App at http://localhost:3000 by signing up with your email and password.

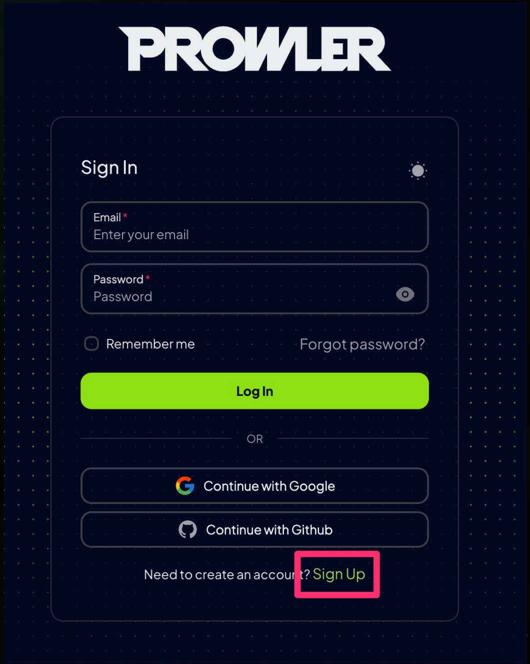
Google and GitHub authentication is only available in Prowler Cloud

NOTE: Containers are built for `linux/amd64`. If your workstation's architecture is different, please set `DOCKER_DEFAULT_PLATFORM=linux/amd64` in your environment or use the `--platform linux/amd64` flag in the docker command.

Lab 21: Sign Up and Log In

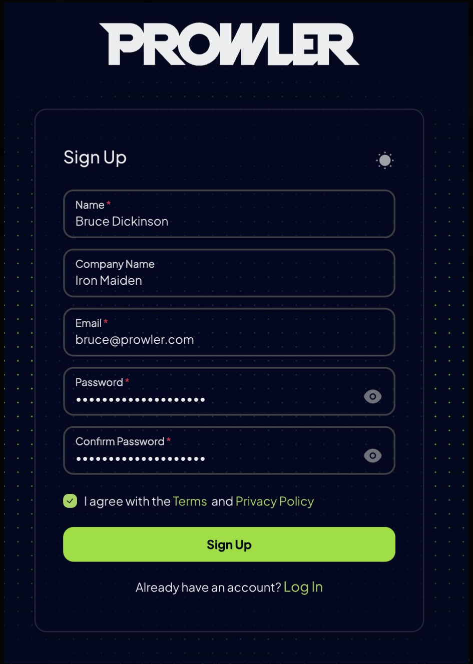
Go to http://localhost:3000 after installing the app. Sign up with your email and password.

Log in with your email and password to start using the Prowler App.



Email * Enter your email

Password * Password



Name * Bruce Dickinson

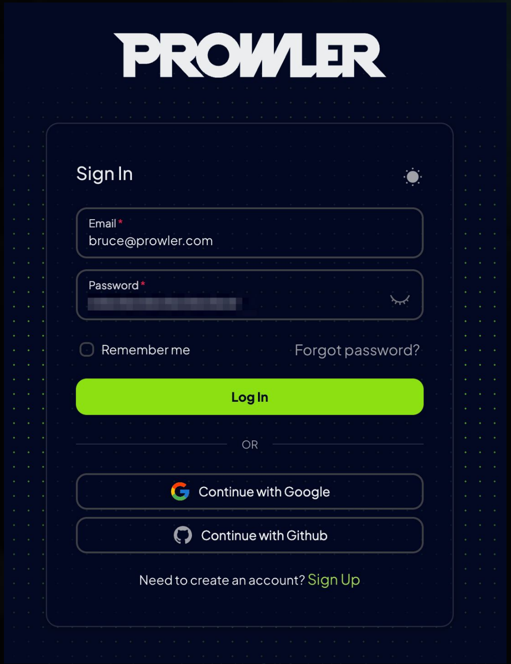
Company Name Iron Maiden

Email * bruce@prowler.com

Password * ••••••••••••••••••••

Confirm Password * ••••••••••••••••••••

☑ I agree with the Terms and Privacy Policy



Email * bruce@prowler.com

Password *

Optional: SAML Single Sign-On (SSO)

Key Features

- **IdP-Initiated SSO**: Users can initiate login from their Identity Provider's dashboard.
- **SP-Initiated SSO**: Users can initiate login directly from the Prowler login page.
- **Just-in-Time Provisioning**: Users from the organization signing into Prowler for the first time will be automatically created.

Prerequisites

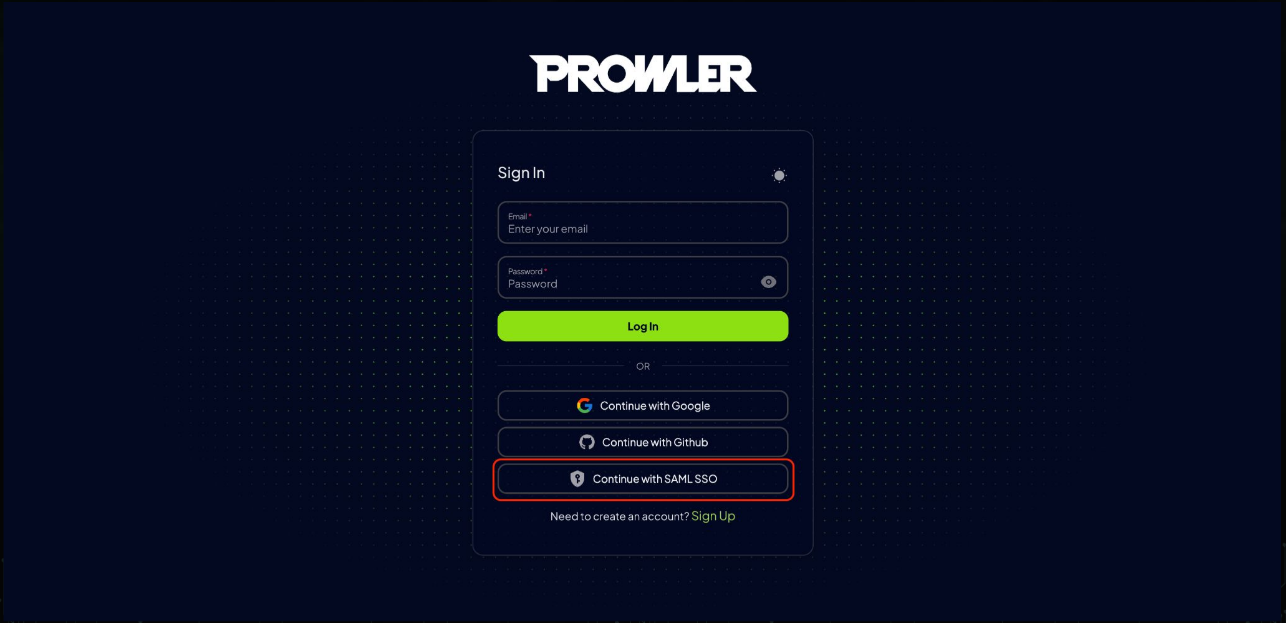
- Administrator access to the Prowler organization is required.
- Administrative access to the SAML 2.0 compliant Identity Provider (e.g., Okta, Azure AD, Google Workspace) is necessary.

Check the configuration steps from the Prowler Docs here

goto.prowler.com/sso-config

Optional: SAML Single Sign-On (SSO)

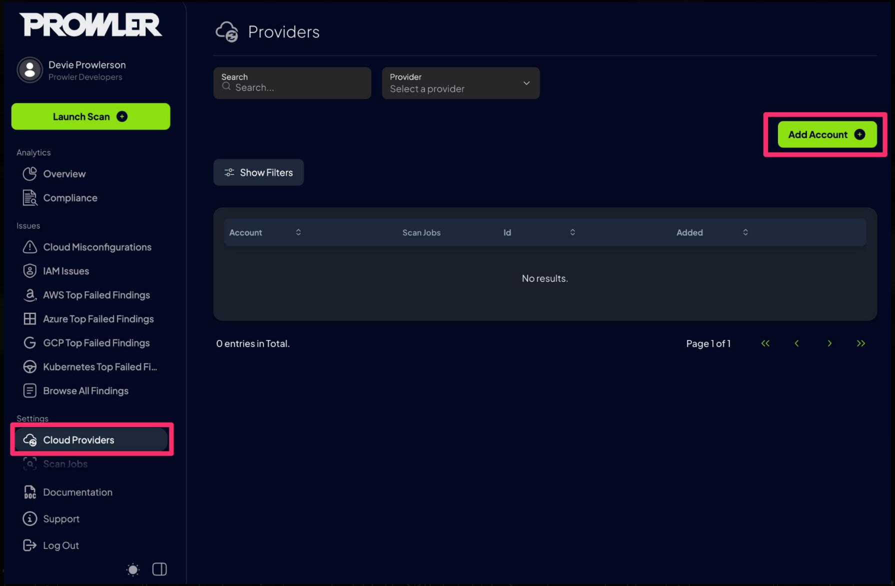
Once **SAML SSO** is enabled, users from the configured domain can sign in by entering their email address on the login page and clicking "**Continue with SAML SSO**". They will be redirected to the IdP to authenticate and then returned to Prowler.



Lab 22: Add a Provider

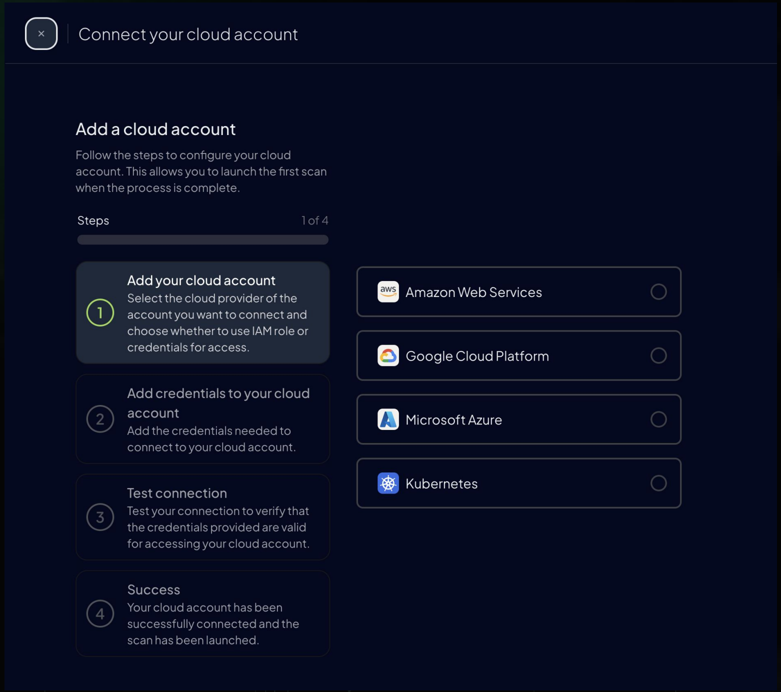
To run your first scan, you need to add a cloud provider account. Prowler App supports AWS, Azure, GCP, and Kubernetes.

1. Navigate to `Settings > Cloud Providers`.
2. Click `Add Account` to set up a new provider and provide your credentials:



Lab 23: Add a Provider

Choose the provider you want to scan from the following options:



× Connect your cloud account

Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 1 of 4

1. Add your cloud account
   Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.
2. Add credentials to your cloud account
   Add the credentials needed to connect to your cloud account.
3. Test connection
   Test your connection to verify that the credentials provided are valid for accessing your cloud account.
4. Success
   Your cloud account has been successfully connected and the scan has been launched.

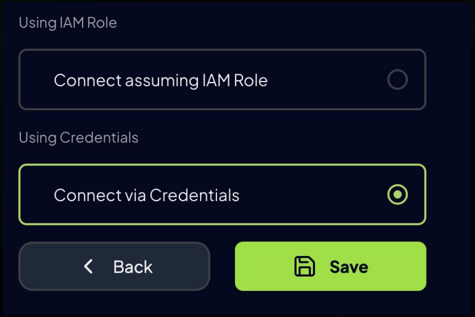
Once you've selected a provider, you need to provide the `Provider UID`:

- AWS: Enter your `AWS Account ID`.
- GCP: Enter your `GCP Project ID`.
- Azure: Enter your `Azure Subscription ID`.
- Kubernetes: Enter your `Kubernetes Cluster context` of your kubeconfig file.

Lab 24: Add a Provider - AWS

Choose one of the following methods to connect with your AWS account:

- Select `Connect via Credentials` to use AWS Access Keys.
  Enter your `Access Key ID`, `Secret Access Key` and optionally a `Session Token`

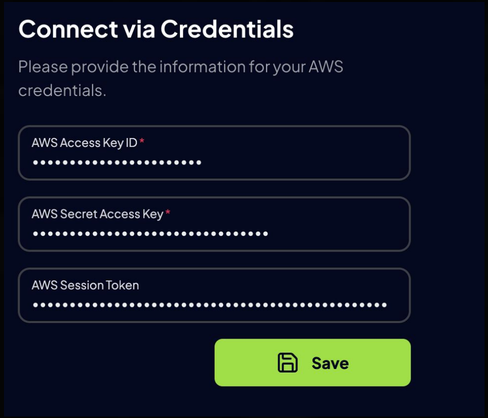


Using IAM Role

Connect assuming IAM Role ○

Using Credentials

Connect via Credentials ●



Connect via Credentials

Please provide the information for your AWS credentials.

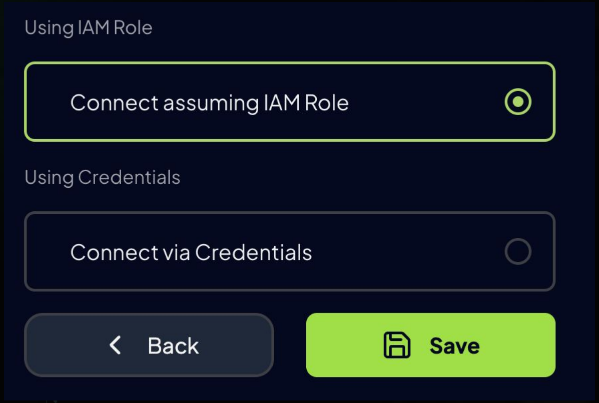
AWS Access Key ID *: ••••••••••••••••••••••

AWS Secret Access Key *: •••••••••••••••••••••••••••••••

AWS Session Token: ••

Lab 25: Add a Provider - AWS

- Select Connect assuming IAM Role:
  Enter the Role ARN and any optional field like the AWS Access Keys to assume the role, the `External ID`, the `Role Session Name` or the `Session Duration`:

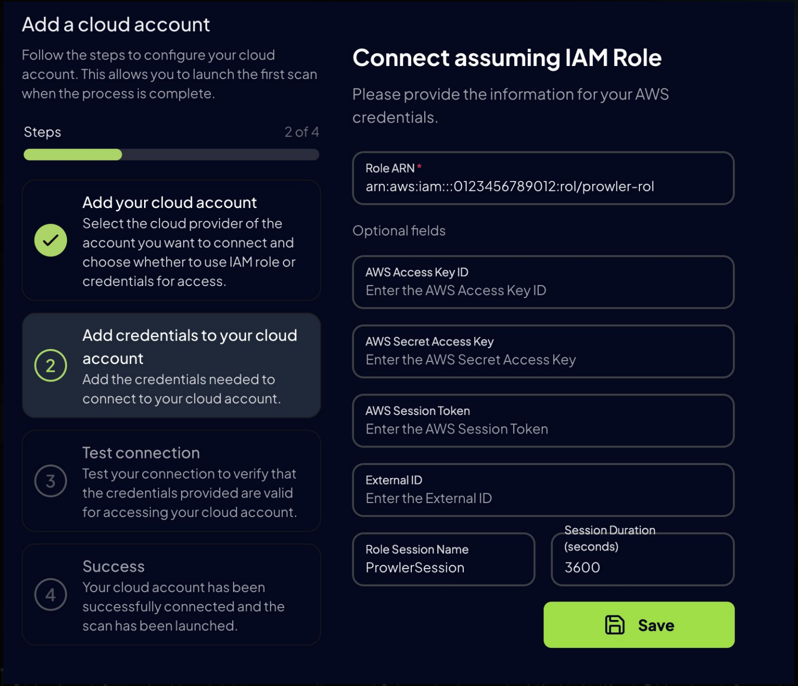


Using IAM Role

Connect assuming IAM Role ●

Using Credentials

Connect via Credentials ○



Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 2 of 4

✓ Add your cloud account
Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.

2 Add credentials to your cloud account
Add the credentials needed to connect to your cloud account.

3 Test connection
Test your connection to verify that the credentials provided are valid for accessing your cloud account.

4 Success
Your cloud account has been successfully connected and the scan has been launched.

Connect assuming IAM Role

Please provide the information for your AWS credentials.

Role ARN *: arn:aws:iam:::0123456789012:rol/prowler-rol

Optional fields

AWS Access Key ID: Enter the AWS Access Key ID

AWS Secret Access Key: Enter the AWS Secret Access Key

AWS Session Token: Enter the AWS Session Token

External ID: Enter the External ID

Role Session Name: ProwlerSession

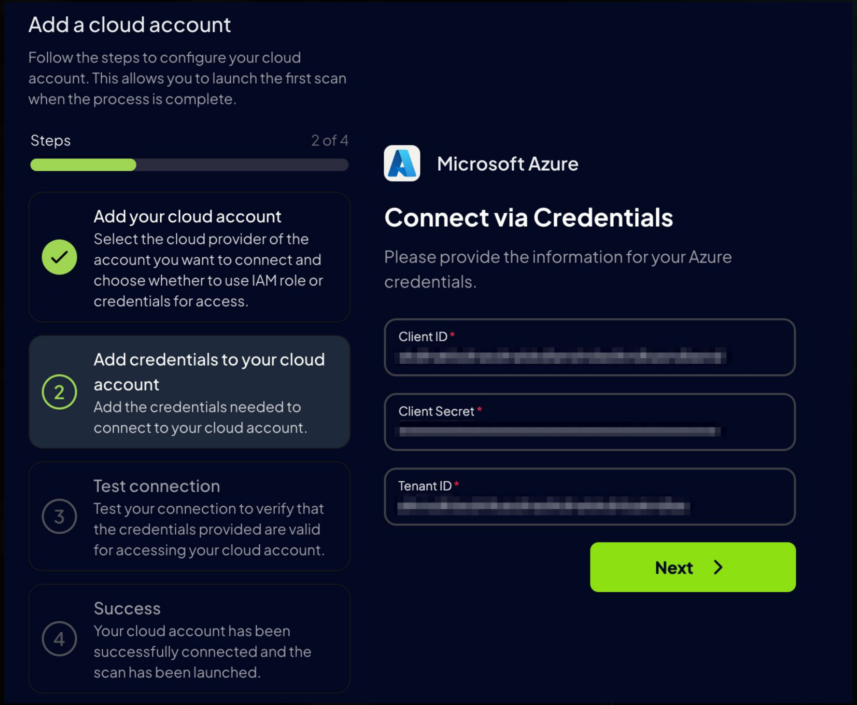
Session Duration (seconds): 3600

Lab 26: Add a Provider - Azure

Prowler App uses Service Principal Application to authenticate with Azure. This service principal should have the following permissions:

- `Directory.Read.All`
- `Policy.Read.All`
- `UserAuthenticationMethod.Read.All`

Then, enter the `Tenant ID`, `Client ID` and `Client Secret` of the created service principal application.



Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 2 of 4

✓ Add your cloud account
Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.

2 Add credentials to your cloud account
Add the credentials needed to connect to your cloud account.

3 Test connection
Test your connection to verify that the credentials provided are valid for accessing your cloud account.

4 Success
Your cloud account has been successfully connected and the scan has been launched.

Microsoft Azure

Connect via Credentials

Please provide the information for your Azure credentials.

Client ID *: [redacted]

Client Secret *: [redacted]

Tenant ID *: [redacted]

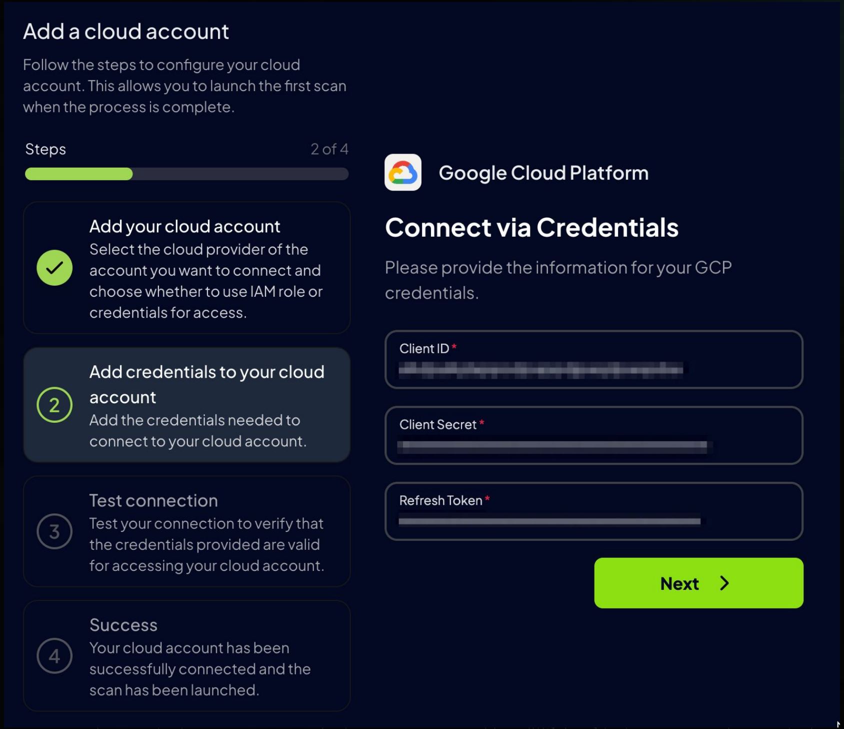
Lab 27: Add a Provider - GCP

To connect your GCP Project, you need to use the Application Default Credentials (ADC) returned by the gcloud CLI. Here's how to set up:

1. Run the following command in your terminal to authenticate with GCP:

   ```
   gcloud auth application-default login
   ```

2. Once authenticated, get the `Client ID`, `Client Secret` and `Refresh Token` from `~/.config/gcloud/application_default_credentials`.
3. Paste the `Client ID`, `Client Secret` and `Refresh Token` into the Prowler App.



Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 2 of 4

✓ **Add your cloud account**
Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.

② **Add credentials to your cloud account**
Add the credentials needed to connect to your cloud account.

③ Test connection
Test your connection to verify that the credentials provided are valid for accessing your cloud account.

④ Success
Your cloud account has been successfully connected and the scan has been launched.

Google Cloud Platform

Connect via Credentials

Please provide the information for your GCP credentials.

Client ID * [redacted]

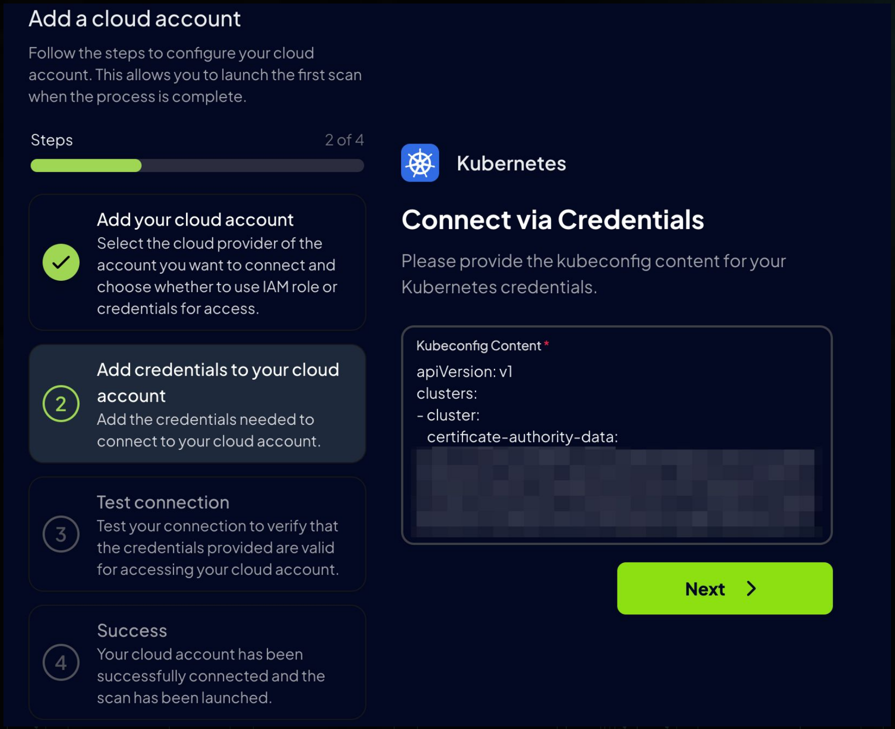
Client Secret * [redacted]

Refresh Token * [redacted]

Lab 28: Add a Provider - Kubernetes

For Kubernetes, Prowler App uses a `kubeconfig file` to authenticate, paste the contents of your `kubeconfig file` into the Kubeconfig content field.

**By default, the kubeconfig file is located at `~/.kube/config`



Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 2 of 4

✓ Add your cloud account
Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.

② Add credentials to your cloud account
Add the credentials needed to connect to your cloud account.

③ Test connection
Test your connection to verify that the credentials provided are valid for accessing your cloud account.

④ Success
Your cloud account has been successfully connected and the scan has been launched.

Kubernetes

Connect via Credentials

Please provide the kubeconfig content for your Kubernetes credentials.

Kubeconfig Content *

```
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
```

[redacted]

Lab 29: Add a Provider - M365

To configure your M365 account, you'll need:

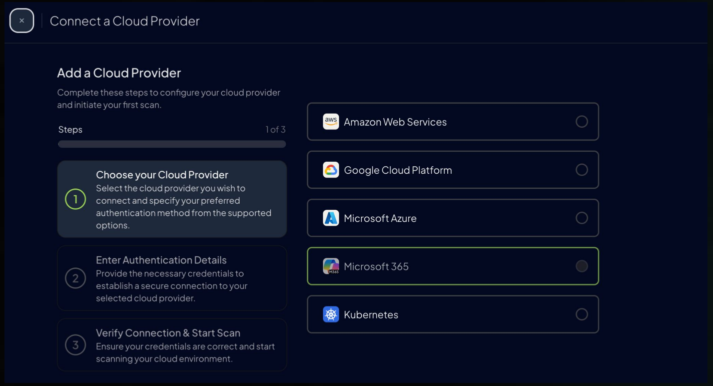
Obtain a domain from the Entra ID portal.

Access Prowler Cloud/App and add a new cloud provider Microsoft 365.

Configure your M365 account:

1. Create the Service Principal app.
2. Grant the required API permissions.
3. Assign the required roles to your user.
4. Add the credentials to Prowler Cloud/App.

Want more info? [Check docs]()



Connect a Cloud Provider

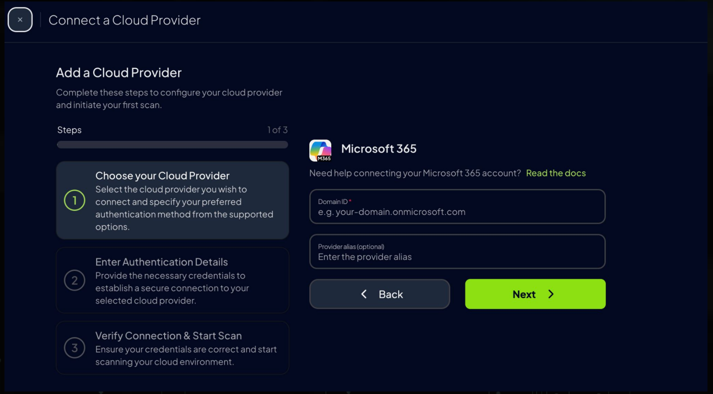
Add a Cloud Provider

Complete these steps to configure your cloud provider and initiate your first scan.

Steps 1 of 3

1. Choose your Cloud Provider
   Select the cloud provider you wish to connect and specify your preferred authentication method from the supported options.
2. Enter Authentication Details
   Provide the necessary credentials to establish a secure connection to your selected cloud provider.
3. Verify Connection & Start Scan
   Ensure your credentials are correct and start scanning your cloud environment.

- Amazon Web Services ○
- Google Cloud Platform ○
- Microsoft Azure ○
- Microsoft 365 ●
- Kubernetes ○



Connect a Cloud Provider

Add a Cloud Provider

Complete these steps to configure your cloud provider and initiate your first scan.

Steps 1 of 3

1. Choose your Cloud Provider
   Select the cloud provider you wish to connect and specify your preferred authentication method from the supported options.
2. Enter Authentication Details
   Provide the necessary credentials to establish a secure connection to your selected cloud provider.
3. Verify Connection & Start Scan
   Ensure your credentials are correct and start scanning your cloud environment.

Microsoft 365

Need help connecting your Microsoft 365 account? Read the docs

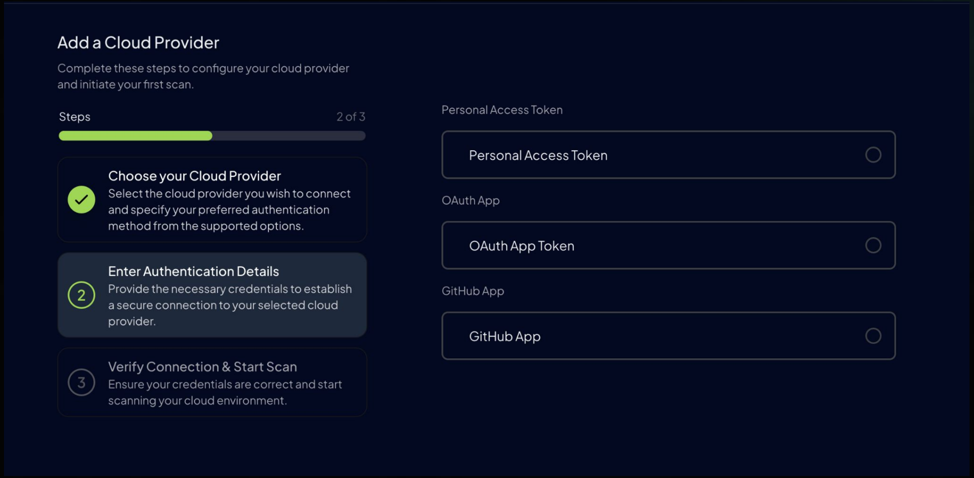
Domain ID *: e.g. your-domain.onmicrosoft.com

Provider alias (optional): Enter the provider alias

Lab 30: Add a Provider - Github

Add your user name and choose the preferred authentication method:

- Personal Access Token (PAT) -> Docs here
- OAuth App Token -> Docs here
- GitHub App Credentials -> Docs here



Add a Cloud Provider

Complete these steps to configure your cloud provider and initiate your first scan.

Steps 2 of 3

✓ Choose your Cloud Provider
Select the cloud provider you wish to connect and specify your preferred authentication method from the supported options.

② Enter Authentication Details
Provide the necessary credentials to establish a secure connection to your selected cloud provider.

③ Verify Connection & Start Scan
Ensure your credentials are correct and start scanning your cloud environment.

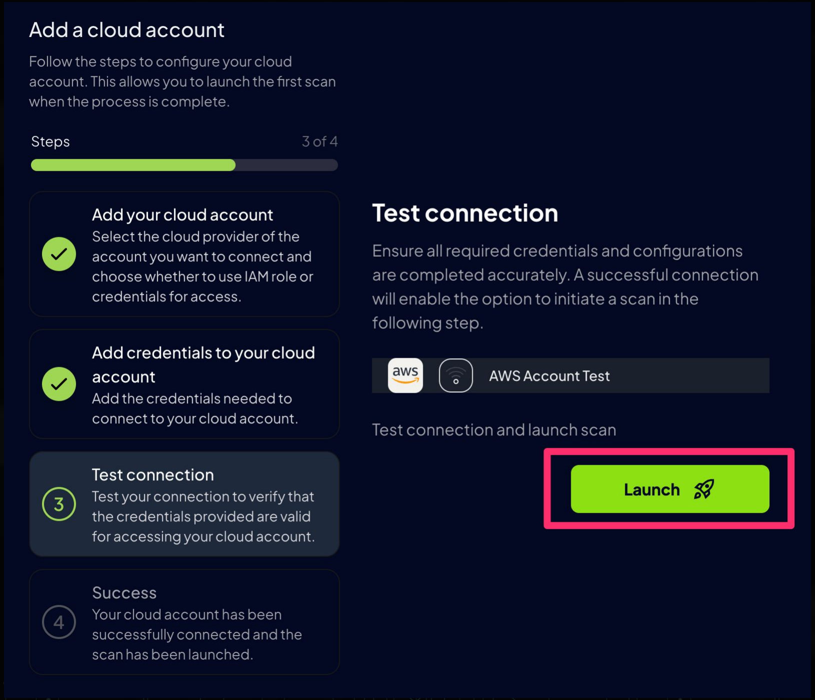
Personal Access Token
Personal Access Token ○

OAuth App
OAuth App Token ○

GitHub App
GitHub App ○

Lab 31: Add a Provider

After adding your credentials of your cloud account, click the `Launch` button to verify that the Prowler App can successfully connect to your provider:



Add a cloud account

Follow the steps to configure your cloud account. This allows you to launch the first scan when the process is complete.

Steps 3 of 4

- ✓ **Add your cloud account** Select the cloud provider of the account you want to connect and choose whether to use IAM role or credentials for access.
- ✓ **Add credentials to your cloud account** Add the credentials needed to connect to your cloud account.
- ③ **Test connection** Test your connection to verify that the credentials provided are valid for accessing your cloud account.
- ④ **Success** Your cloud account has been successfully connected and the scan has been launched.

Test connection

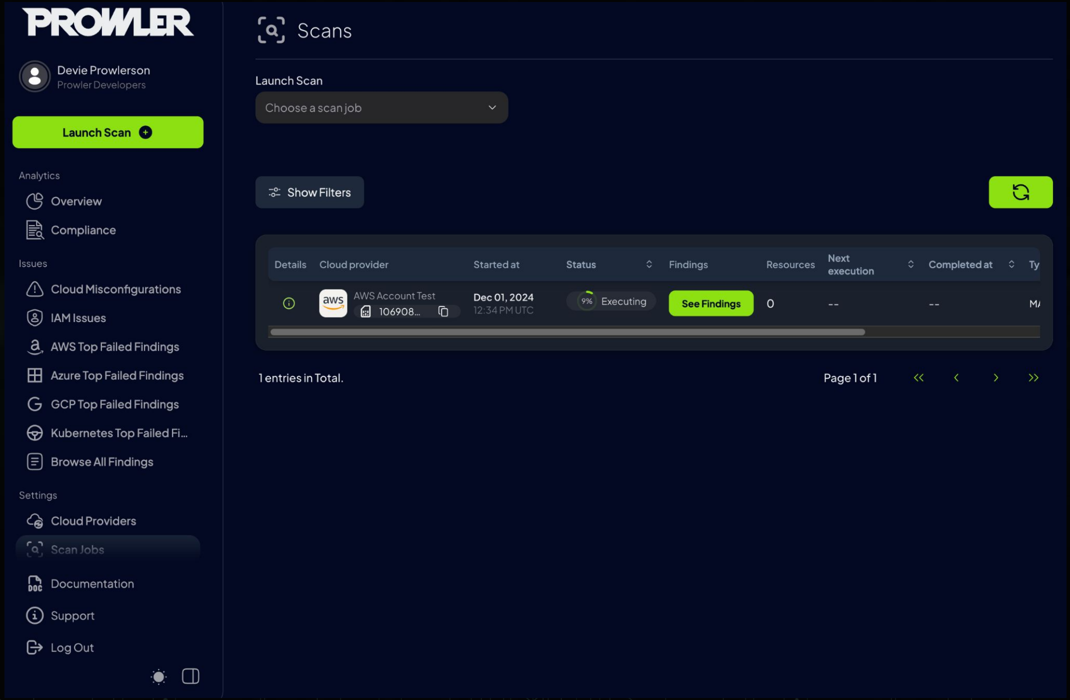
Ensure all required credentials and configurations are completed accurately. A successful connection will enable the option to initiate a scan in the following step.

aws AWS Account Test

Test connection and launch scan

Lab 31: Analyze findings

Once the scan has started, you can track the progress of your scan in the `Scans` section:



Details	Cloud provider	Started at	Status	Findings	Resources	Next execution	Completed at	Ty
ⓘ	aws AWS Account Test 106908...	Dec 01, 2024 12:34 PM UTC	9% Executing	See Findings	0	--	--	M/

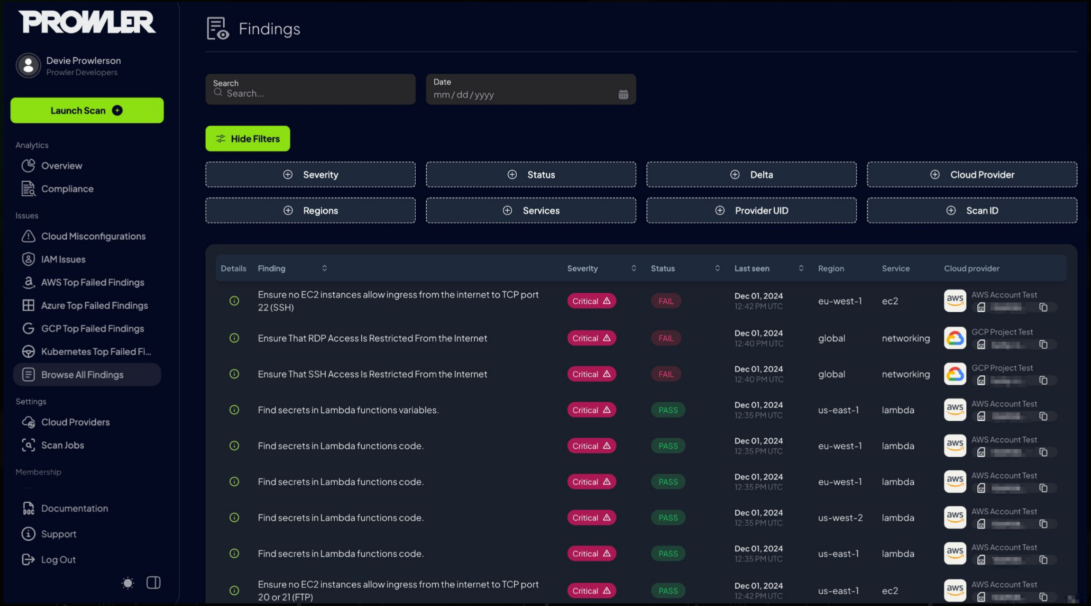
1 entries in Total.

Page 1 of 1

Lab 32: Analyze findings

While the scan is running, start exploring the findings in these sections:

- Browse All Findings: Detailed list of findings detected, where you can filter by severity, service, and more.

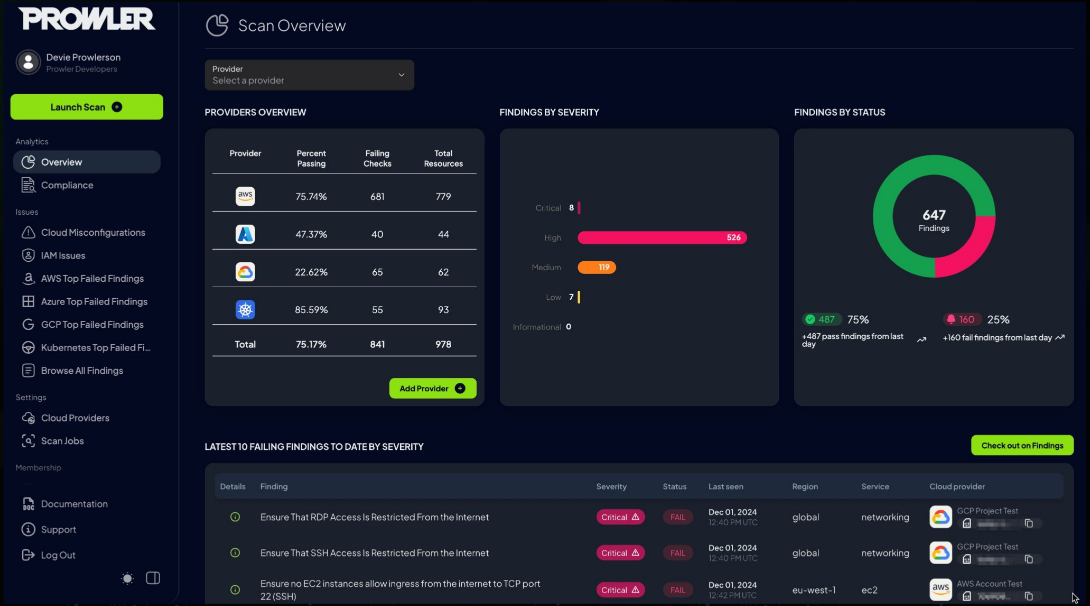


Details	Finding	Severity	Status	Last seen	Region	Service	Cloud provider
ⓘ	Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)	Critical ⚠	FAIL	Dec 01, 2024 12:42 PM UTC	eu-west-1	ec2	aws AWS Account Test [redacted]
ⓘ	Ensure That RDP Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Ensure That SSH Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Find secrets in Lambda functions variables.	Critical ⚠	PASS	Dec 01, 2024 12:35 PM UTC	us-east-1	lambda	aws AWS Account Test [redacted]
ⓘ	Find secrets in Lambda functions code.	Critical ⚠	PASS	Dec 01, 2024 12:35 PM UTC	eu-west-1	lambda	aws AWS Account Test [redacted]
ⓘ	Find secrets in Lambda functions code.	Critical ⚠	PASS	Dec 01, 2024 12:35 PM UTC	eu-west-1	lambda	aws AWS Account Test [redacted]
ⓘ	Find secrets in Lambda functions code.	Critical ⚠	PASS	Dec 01, 2024 12:35 PM UTC	us-west-2	lambda	aws AWS Account Test [redacted]
ⓘ	Find secrets in Lambda functions code.	Critical ⚠	PASS	Dec 01, 2024 12:35 PM UTC	us-east-1	lambda	aws AWS Account Test [redacted]
ⓘ	Ensure no EC2 instances allow ingress from the internet to TCP port 20 or 21 (FTP)	Critical ⚠	PASS	Dec 01, 2024 12:42 PM UTC	us-east-1	ec2	aws AWS Account Test [redacted]

Lab 32: Analyze findings

While the scan is running, start exploring the findings in these sections:

- Overview: High-level summary of the scans.



Provider
Select a provider

PROVIDERS OVERVIEW

Provider	Percent Passing	Failing Checks	Total Resources
aws	75.74%	681	779
	47.37%	40	44
	22.62%	65	62
	85.59%	55	93
Total	75.17%	841	978

FINDINGS BY SEVERITY

FINDINGS BY STATUS

647
Findings
487 75%
+487 pass findings from last day
160 25%
+160 fail findings from last day

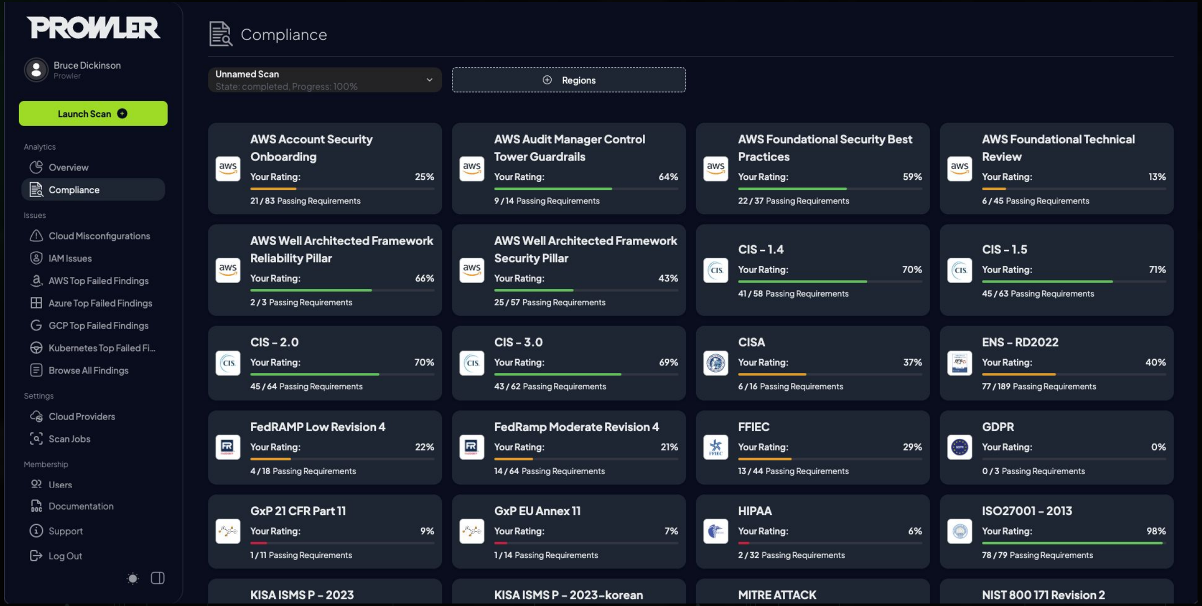
LATEST 10 FAILING FINDINGS TO DATE BY SEVERITY

Details	Finding	Severity	Status	Last seen	Region	Service	Cloud provider
ⓘ	Ensure That RDP Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Ensure That SSH Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)	Critical ⚠	FAIL	Dec 01, 2024 12:42 PM UTC	eu-west-1	ec2	aws AWS Account Test [redacted]

Lab 32: Analyze findings

While the scan is running, start exploring the findings in these sections:

- Compliance: Insights into compliance status.

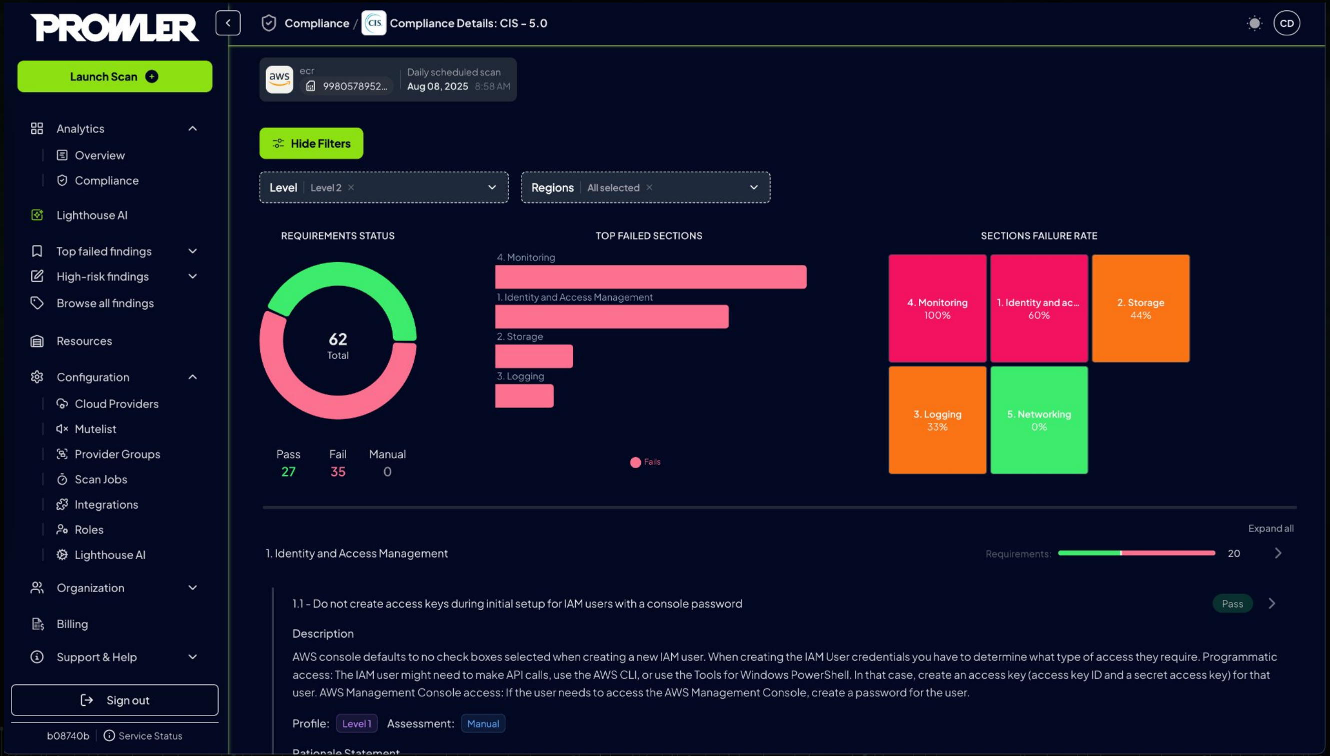


Unnamed Scan
State: completed, Progress: 100%

AWS Account Security Onboarding	Your Rating: 25%	21 / 83 Passing Requirements
AWS Audit Manager Control Tower Guardrails	Your Rating: 64%	9 / 14 Passing Requirements
AWS Foundational Security Best Practices	Your Rating: 59%	22 / 37 Passing Requirements
AWS Foundational Technical Review	Your Rating: 13%	6 / 45 Passing Requirements
AWS Well Architected Framework Reliability Pillar	Your Rating: 66%	2 / 3 Passing Requirements
AWS Well Architected Framework Security Pillar	Your Rating: 43%	25 / 57 Passing Requirements
CIS - 1.4	Your Rating: 70%	41 / 58 Passing Requirements
CIS - 1.5	Your Rating: 71%	45 / 63 Passing Requirements
CIS - 2.0	Your Rating: 70%	45 / 64 Passing Requirements
CIS - 3.0	Your Rating: 69%	43 / 62 Passing Requirements
CISA	Your Rating: 37%	6 / 16 Passing Requirements
ENS - RD2022	Your Rating: 40%	77 / 189 Passing Requirements
FedRAMP Low Revision 4	Your Rating: 22%	4 / 18 Passing Requirements
FedRamp Moderate Revision 4	Your Rating: 21%	14 / 64 Passing Requirements
FFIEC	Your Rating: 29%	13 / 44 Passing Requirements
GDPR	Your Rating: 0%	0 / 3 Passing Requirements
GxP 21 CFR Part 11	Your Rating: 9%	1 / 11 Passing Requirements
GxP EU Annex 11	Your Rating: 7%	1 / 14 Passing Requirements
HIPAA	Your Rating: 6%	2 / 32 Passing Requirements
ISO27001 - 2013	Your Rating: 98%	78 / 79 Passing Requirements
KISA ISMS P - 2023		
KISA ISMS P - 2023-korean		
MITRE ATTACK		
NIST 800 171 Revision 2		

Lab 33: Compliance in Prowler App

Check your “favorite” compliance and drill down thru requirements:



Compliance / Compliance Details: CIS - 5.0

aws ecr 9980578952... Daily scheduled scan Aug 08, 2025 8:58 AM

Level: Level 2

Regions: All selected

REQUIREMENTS STATUS

62 Total

Pass 27 Fail 35 Manual 0

TOP FAILED SECTIONS

SECTIONS FAILURE RATE

1. Identity and Access Management — Requirements: 20

1.1 - Do not create access keys during initial setup for IAM users with a console password — Pass

Description

AWS console defaults to no check boxes selected when creating a new IAM user. When creating the IAM User credentials you have to determine what type of access they require. Programmatic access: The IAM user might need to make API calls, use the AWS CLI, or use the Tools for Windows PowerShell. In that case, create an access key (access key ID and a secret access key) for that user. AWS Management Console access: If the user needs to access the AWS Management Console, create a password for the user.

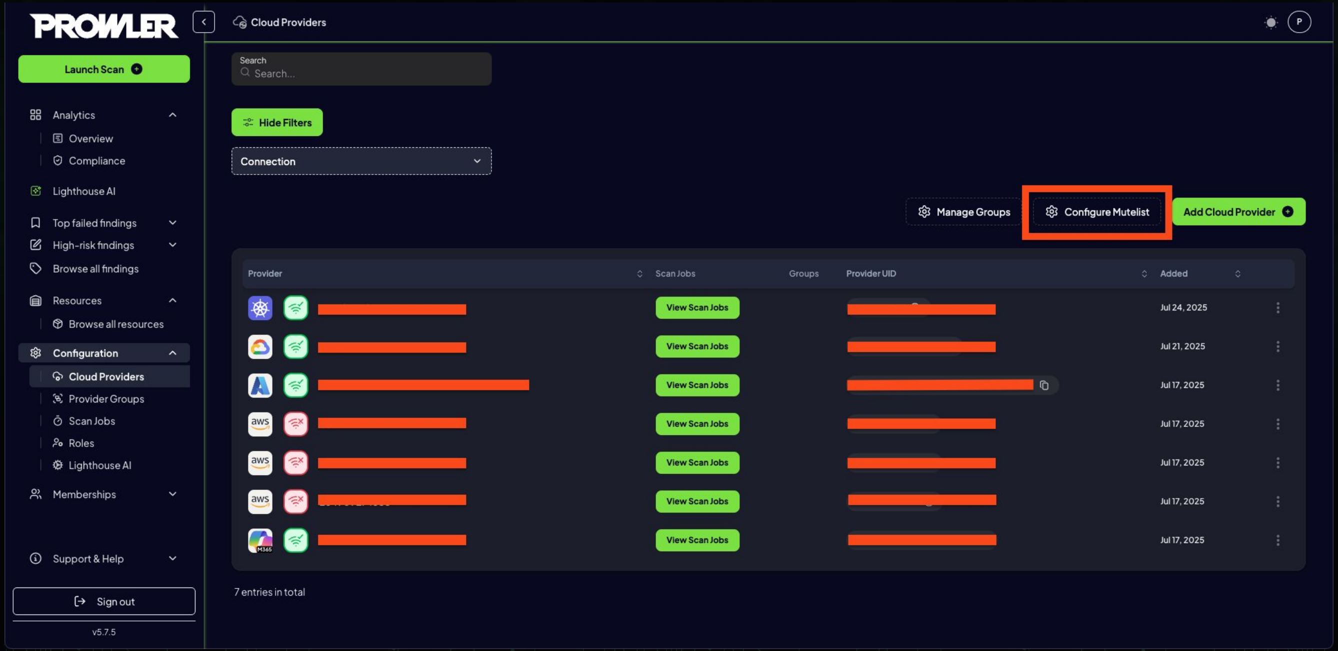
Profile: Level 1 Assessment: Manual

Rationale Statement

Optional: Mutelisting in Prowler App

Prowler App allows users to mute specific findings to focus on the most critical security issues.

Go to **Cloud Providers** page and click on

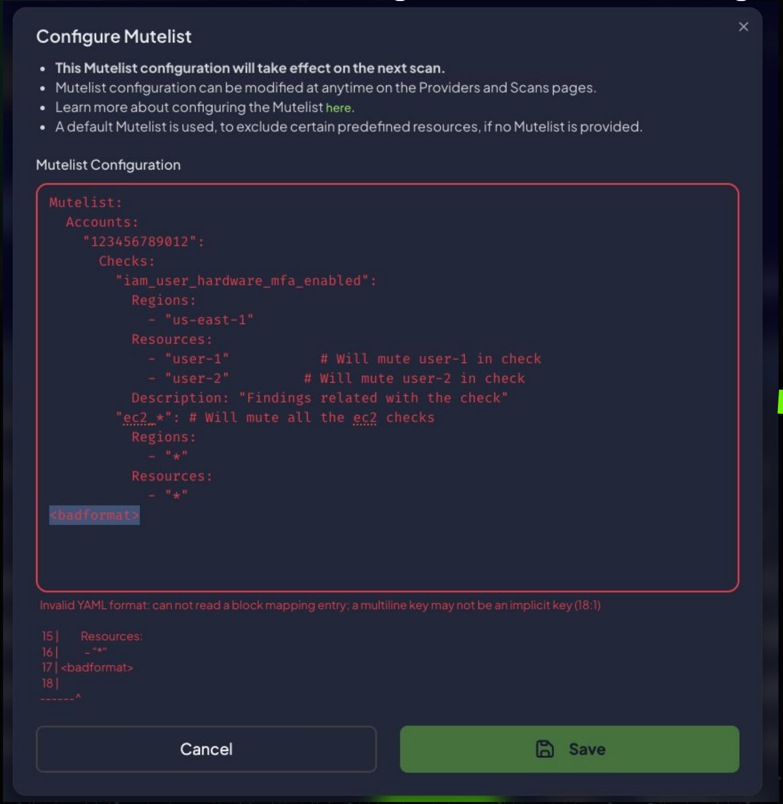


Provider	Scan Jobs	Groups	Provider UID	Added
[redacted]	View Scan Jobs		[redacted]	Jul 24, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 21, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 17, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 17, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 17, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 17, 2025
[redacted]	View Scan Jobs		[redacted]	Jul 17, 2025

7 entries in total

Optional: Mutelisting in Prowler App

Fill the Mutelist config with a correct configuration.



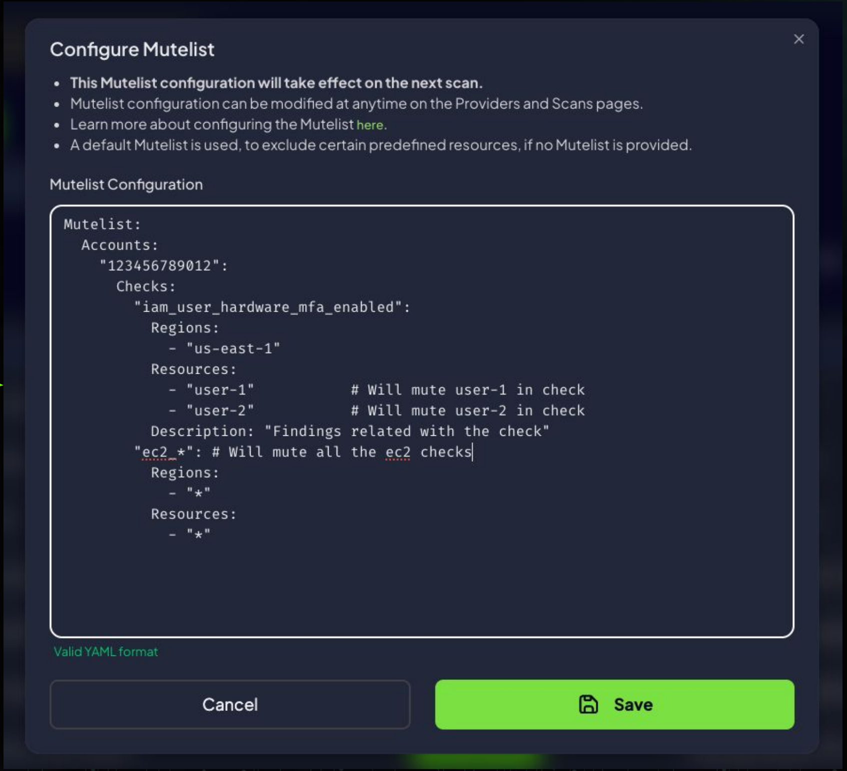
Configure Mutelist

- **This Mutelist configuration will take effect on the next scan.**
- Mutelist configuration can be modified at anytime on the Providers and Scans pages.
- Learn more about configuring the Mutelist here.
- A default Mutelist is used, to exclude certain predefined resources, if no Mutelist is provided.

Mutelist Configuration

```
Mutelist:
  Accounts:
    "123456789012":
      Checks:
        "iam_user_hardware_mfa_enabled":
          Regions:
            - "us-east-1"
          Resources:
            - "user-1"           # Will mute user-1 in check
            - "user-2"          # Will mute user-2 in check
          Description: "Findings related with the check"
        "ec2_*": # Will mute all the ec2 checks
          Regions:
            - "*"
          Resources:
            - "*"
<badformat>
```

```
Invalid YAML format: can not read a block mapping entry; a multiline key may not be an implicit key (18:1)

15 |          Resources:
16 |            - "*"
17 | <badformat>
18 |
-------^
```



Configure Mutelist

- **This Mutelist configuration will take effect on the next scan.**
- Mutelist configuration can be modified at anytime on the Providers and Scans pages.
- Learn more about configuring the Mutelist here.
- A default Mutelist is used, to exclude certain predefined resources, if no Mutelist is provided.

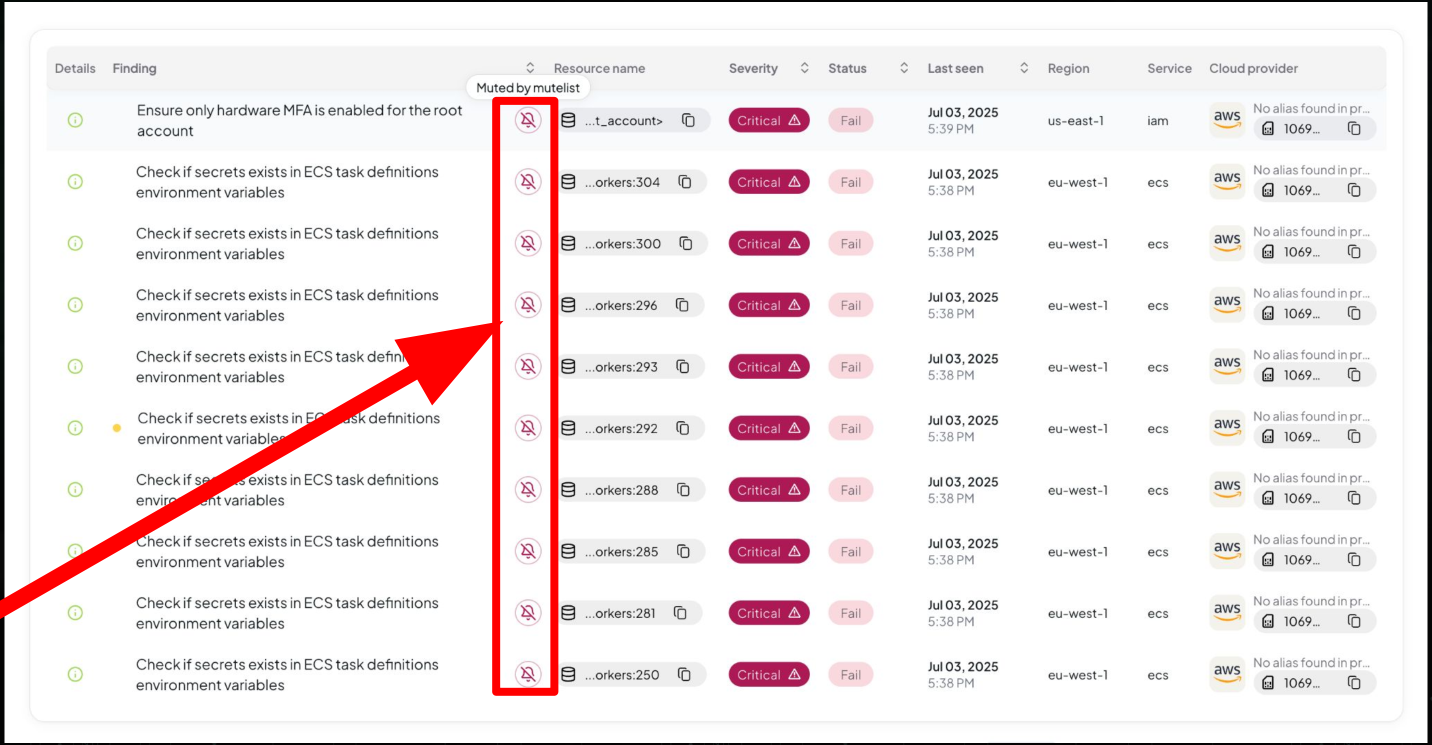
Mutelist Configuration

```
Mutelist:
  Accounts:
    "123456789012":
      Checks:
        "iam_user_hardware_mfa_enabled":
          Regions:
            - "us-east-1"
          Resources:
            - "user-1"          # Will mute user-1 in check
            - "user-2"          # Will mute user-2 in check
          Description: "Findings related with the check"
        "ec2_*": # Will mute all the ec2 checks
          Regions:
            - "*"
          Resources:
            - "*"
```

Valid YAML format

Optional: Mutelisting in Prowler App

Check for muted findings after the scan.

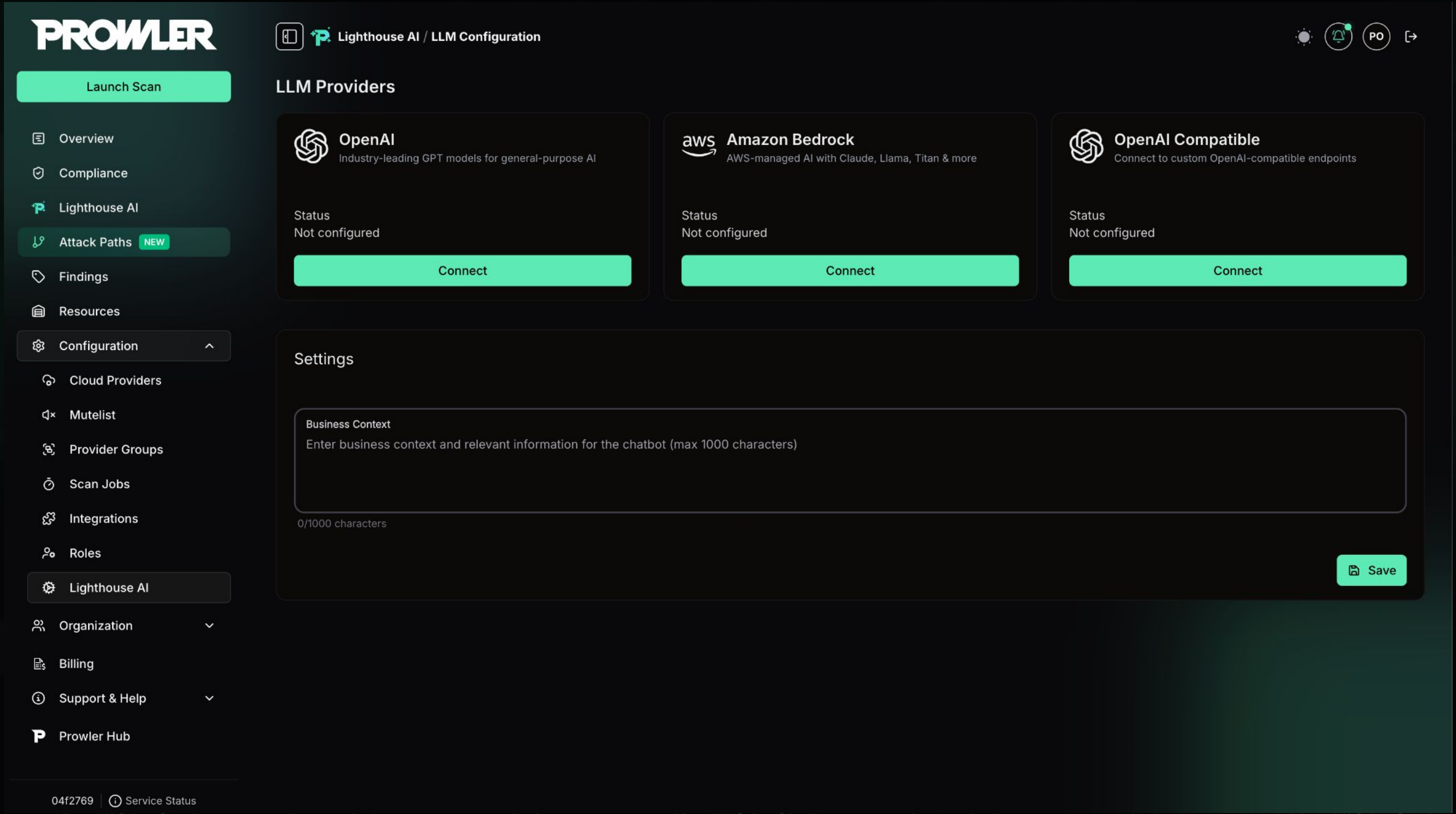


Muted by mutelist

Details	Finding		Resource name	Severity	Status	Last seen	Region	Service	Cloud provider
ⓘ	Ensure only hardware MFA is enabled for the root account	🔕	...t_account>	Critical ⚠	Fail	Jul 03, 2025 5:39 PM	us-east-1	iam	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:304	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:300	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:296	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task defini environment variables	🔕	...orkers:293	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	● Check if secrets exists in E sk definitions environment variable	🔕	...orkers:292	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if se exists in ECS task definitions enviro nt variables	🔕	...orkers:288	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:285	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:281	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...
ⓘ	Check if secrets exists in ECS task definitions environment variables	🔕	...orkers:250	Critical ⚠	Fail	Jul 03, 2025 5:38 PM	eu-west-1	ecs	aws No alias found in pr... 1069...

APP

Lab X - Lighthouse AI



Lighthouse AI / LLM Configuration

LLM Providers

OpenAI
Industry-leading GPT models for general-purpose AI
Status
Not configured

Amazon Bedrock
AWS-managed AI with Claude, Llama, Titan & more
Status
Not configured

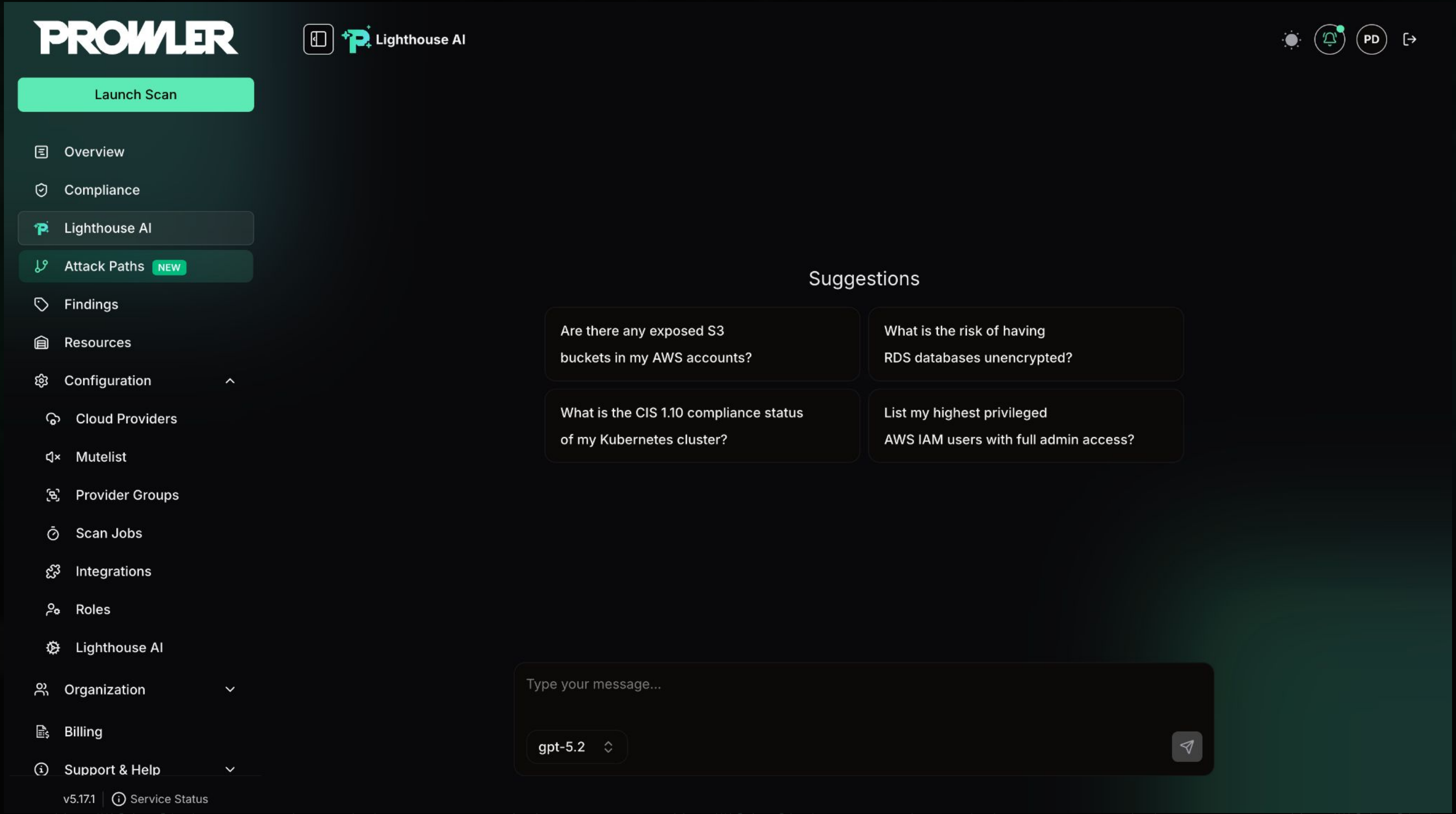
OpenAI Compatible
Connect to custom OpenAI-compatible endpoints
Status
Not configured

Settings

Business Context
Enter business context and relevant information for the chatbot (max 1000 characters)
0/1000 characters

APP

Lab X - Lighthouse AI



Suggestions

Are there any exposed S3 buckets in my AWS accounts?

What is the risk of having RDS databases unencrypted?

What is the CIS 1.10 compliance status of my Kubernetes cluster?

List my highest privileged AWS IAM users with full admin access?

Type your message...

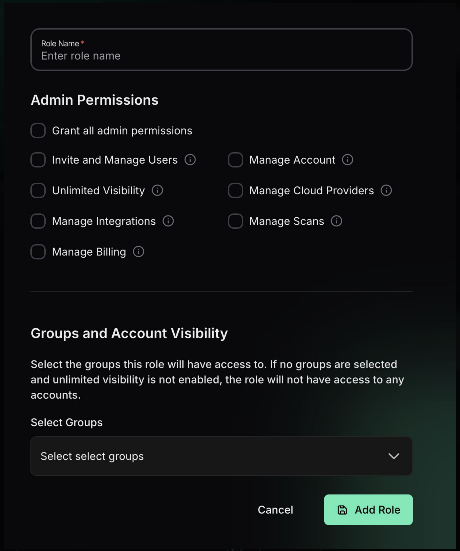
gpt-5.2

APP

Lab X - RBAC

Manage the users from your tenant.

- Assign roles
- Permission scope



Role Name *
Enter role name

Admin Permissions

☐ Grant all admin permissions

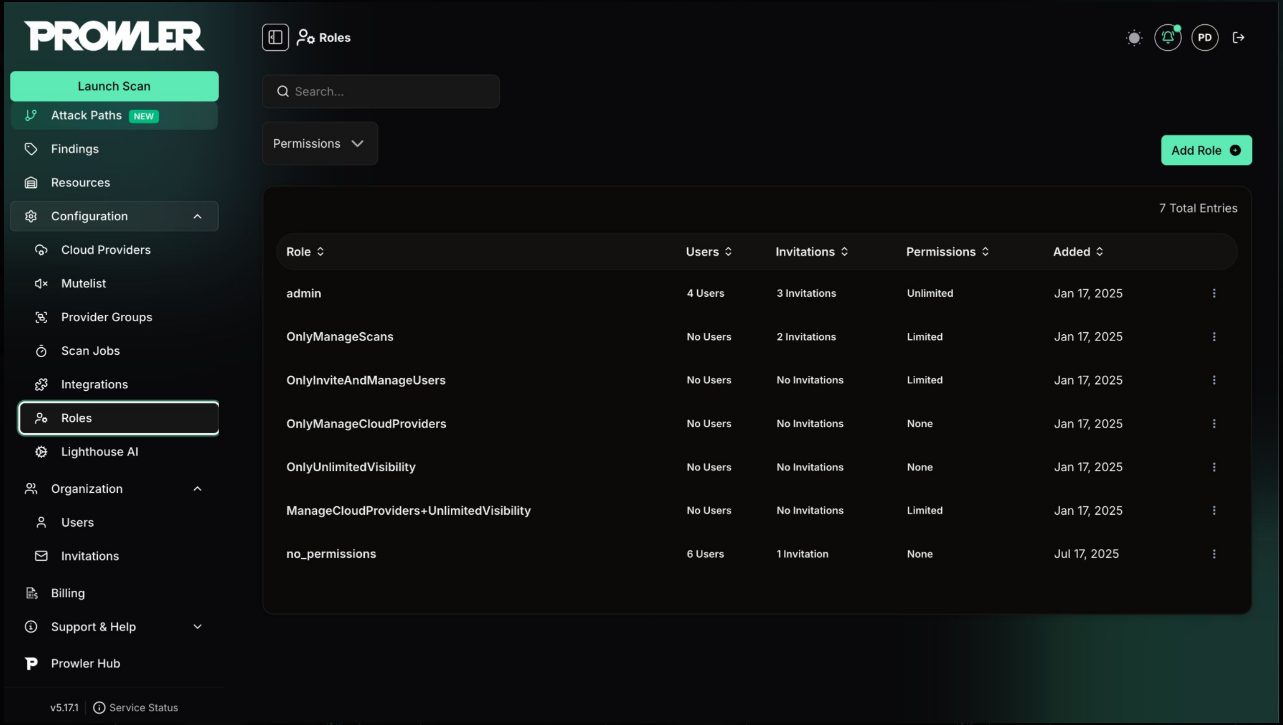
☐ Invite and Manage Users ⓘ
☐ Manage Account ⓘ
☐ Unlimited Visibility ⓘ
☐ Manage Cloud Providers ⓘ
☐ Manage Integrations ⓘ
☐ Manage Scans ⓘ
☐ Manage Billing ⓘ

Groups and Account Visibility

Select the groups this role will have access to. If no groups are selected and unlimited visibility is not enabled, the role will not have access to any accounts.

Select Groups

Select select groups

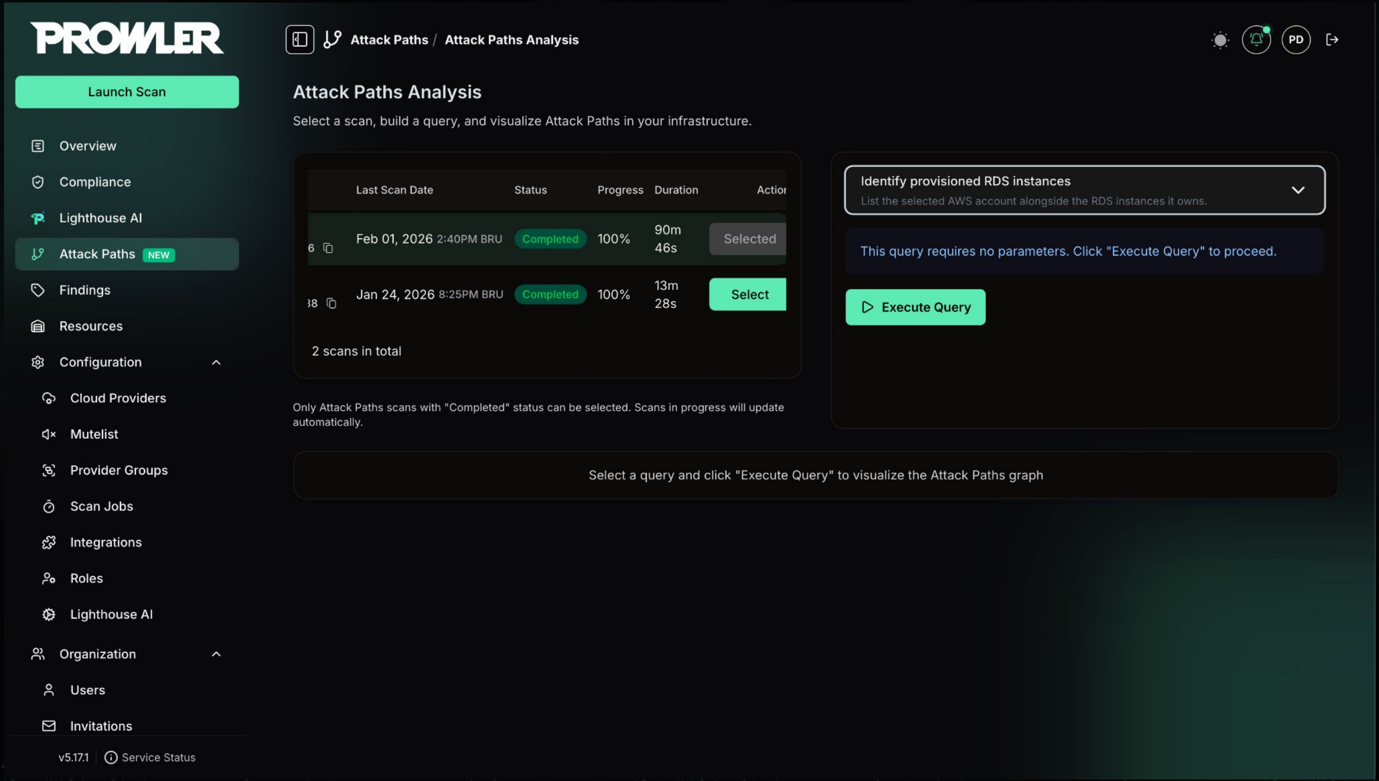


7 Total Entries

Role	Users	Invitations	Permissions	Added
admin	4 Users	3 Invitations	Unlimited	Jan 17, 2025
OnlyManageScans	No Users	2 Invitations	Limited	Jan 17, 2025
OnlyInviteAndManageUsers	No Users	No Invitations	Limited	Jan 17, 2025
OnlyManageCloudProviders	No Users	No Invitations	None	Jan 17, 2025
OnlyUnlimitedVisibility	No Users	No Invitations	None	Jan 17, 2025
ManageCloudProviders+UnlimitedVisibility	No Users	No Invitations	Limited	Jan 17, 2025
no_permissions	6 Users	1 Invitation	None	Jul 17, 2025

APP

Lab X - Attack Path



Attack Paths Analysis

Select a scan, build a query, and visualize Attack Paths in your infrastructure.

	Last Scan Date	Status	Progress	Duration	Action
6	Feb 01, 2026 2:40PM BRU	Completed	100%	90m 46s	Selected
38	Jan 24, 2026 8:25PM BRU	Completed	100%	13m 28s	Select

2 scans in total

Only Attack Paths scans with "Completed" status can be selected. Scans in progress will update automatically.

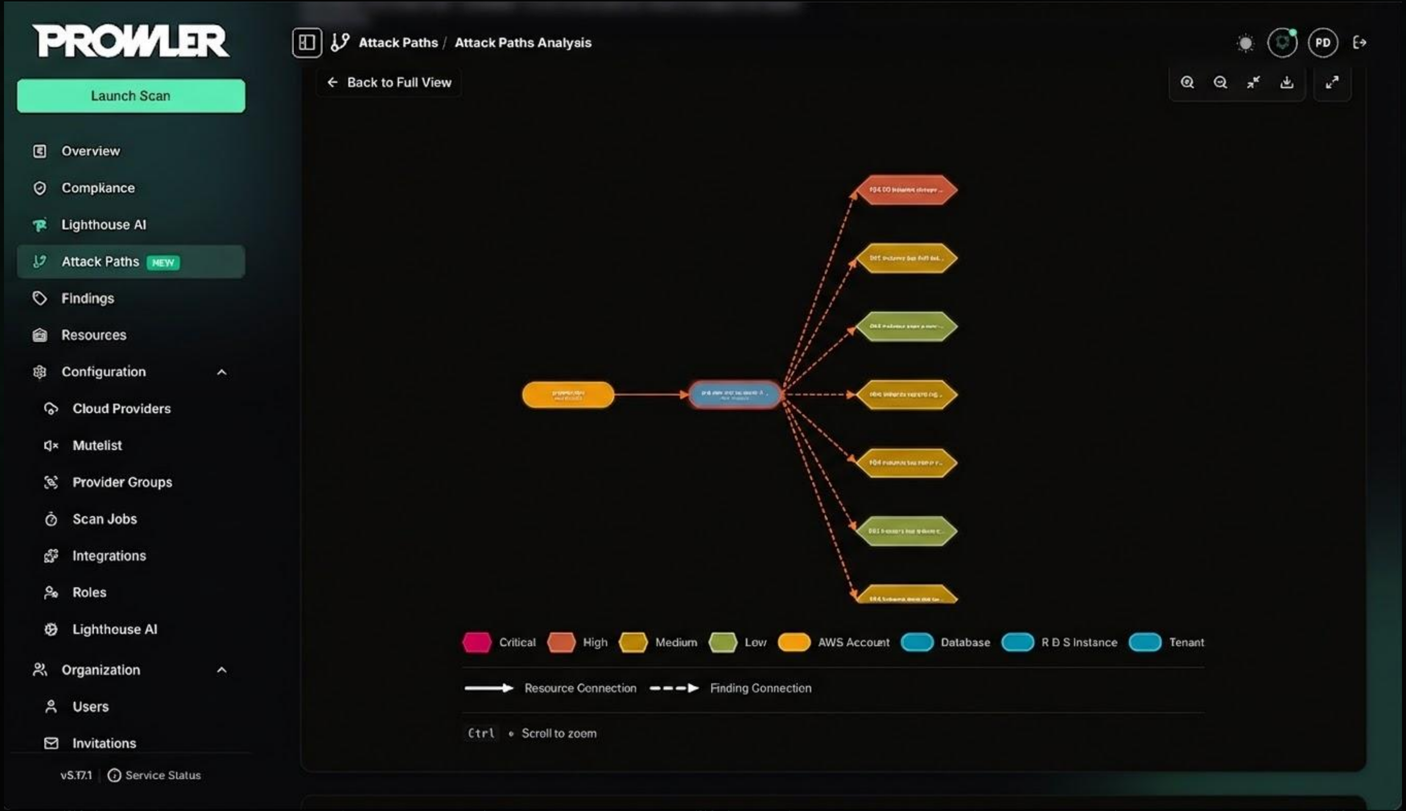
Identify provisioned RDS instances
List the selected AWS account alongside the RDS instances it owns.

This query requires no parameters. Click "Execute Query" to proceed.

Select a query and click "Execute Query" to visualize the Attack Paths graph

APP

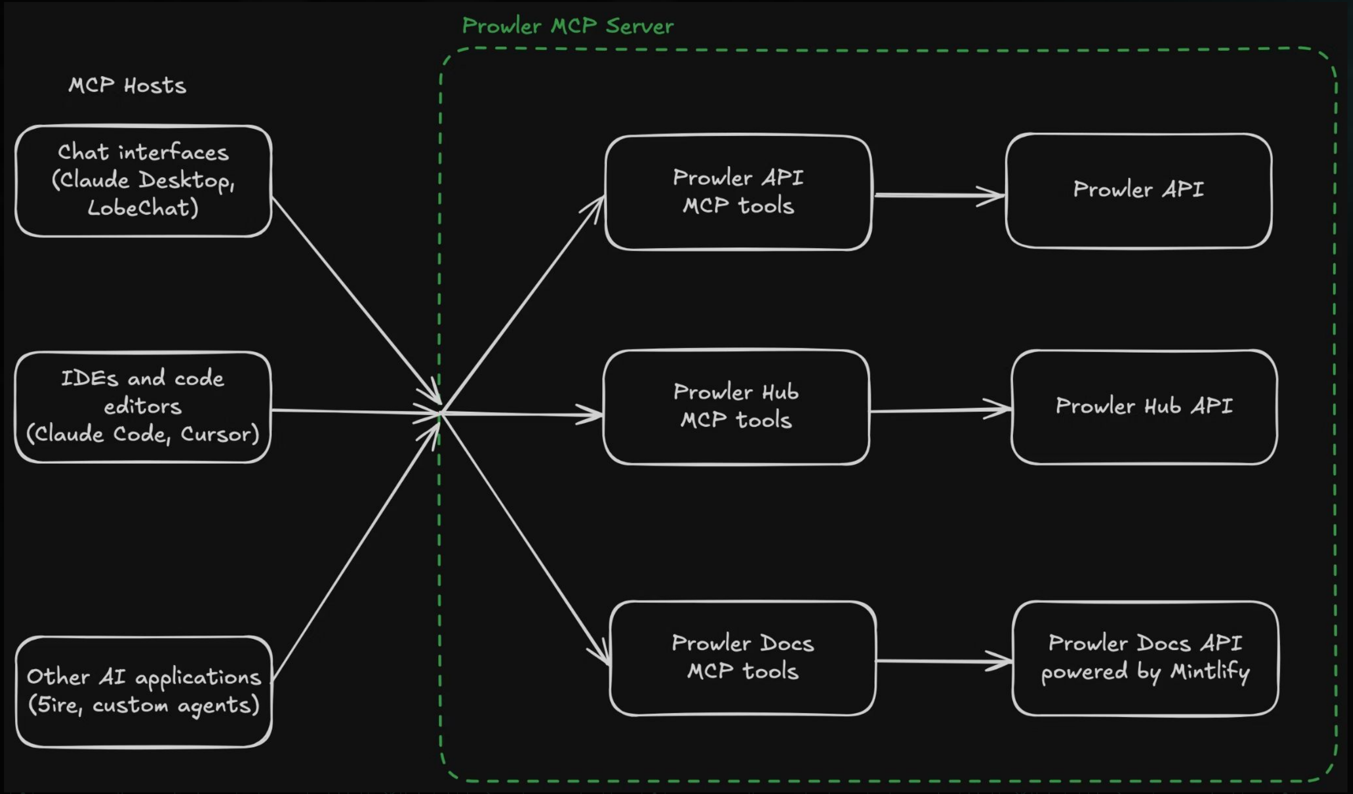
Lab X - Attack Path

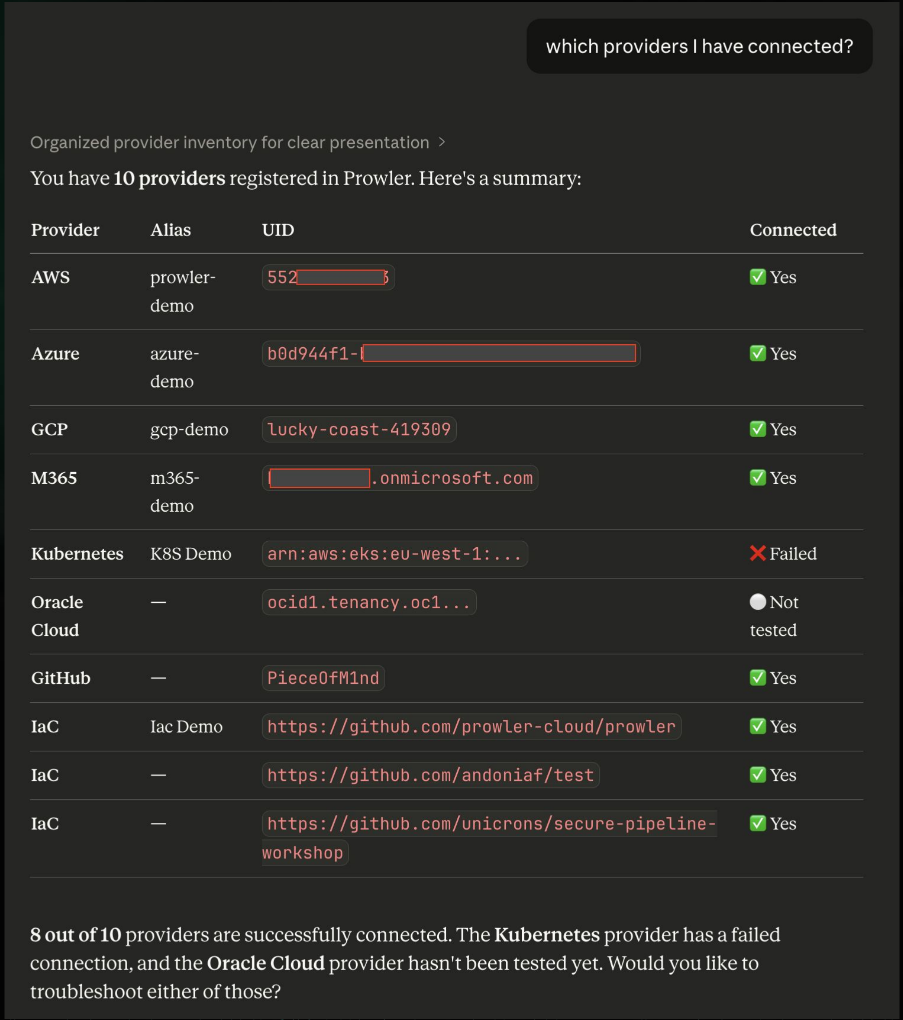


PROWLER

MCP

- ✓ Prowler Cloud / App
- ✓ Prowler Hub
- ✓ Prowler Docs


Prowler MCP Server
MCP Hosts
Chat interfaces (Claude Desktop, LobeChat)
IDEs and code editors (Claude Code, Cursor)
Other AI applications (5ire, custom agents)
Prowler API MCP tools
Prowler Hub MCP tools
Prowler Docs MCP tools
Prowler API
Prowler Hub API
Prowler Docs API powered by Mintlify



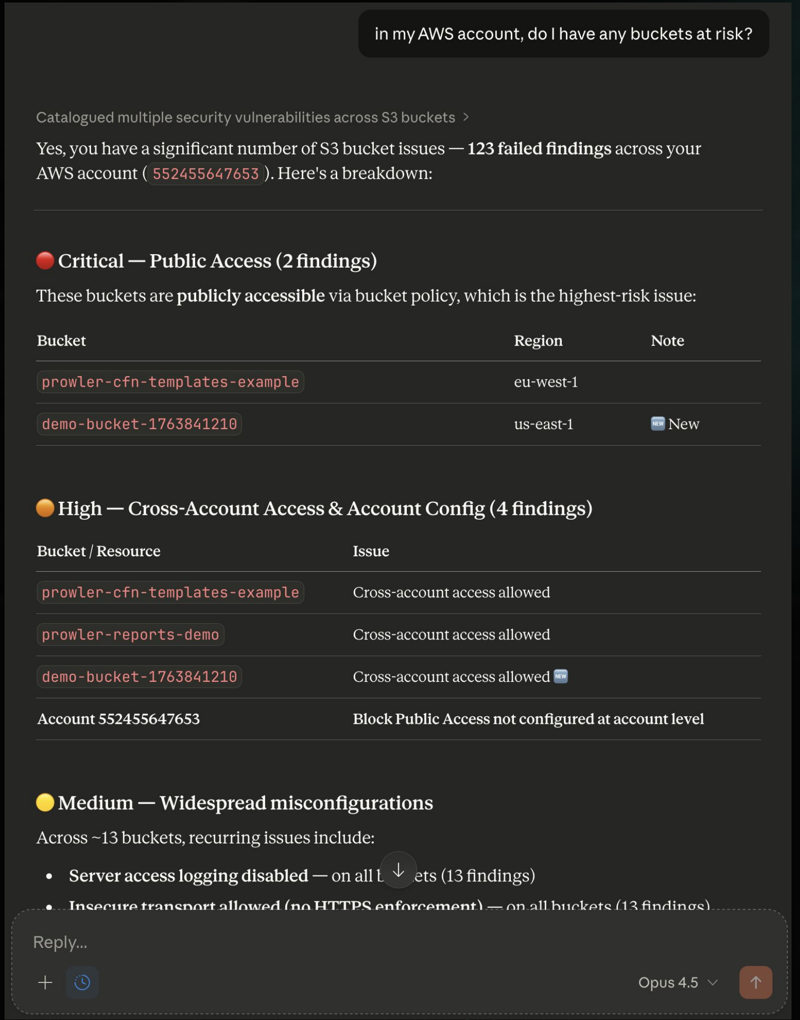
which providers I have connected?

Organized provider inventory for clear presentation >

You have **10 providers** registered in Prowler. Here's a summary:

Provider	Alias	UID	Connected
AWS	prowler-demo	`552[redacted]`	✅ Yes
Azure	azure-demo	`b0d944f1-[redacted]`	✅ Yes
GCP	gcp-demo	`lucky-coast-419309`	✅ Yes
M365	m365-demo	`[redacted].onmicrosoft.com`	✅ Yes
Kubernetes	K8S Demo	`arn:aws:eks:eu-west-1:...`	❌ Failed
Oracle Cloud	—	`ocid1.tenancy.oc1...`	⚪ Not tested
GitHub	—	`PieceOfM1nd`	✅ Yes
IaC	Iac Demo	`https://github.com/prowler-cloud/prowler`	✅ Yes
IaC	—	`https://github.com/andoniaf/test`	✅ Yes
IaC	—	`https://github.com/unicrons/secure-pipeline-workshop`	✅ Yes

8 out of 10 providers are successfully connected. The **Kubernetes** provider has a failed connection, and the **Oracle Cloud** provider hasn't been tested yet. Would you like to troubleshoot either of those?



in my AWS account, do I have any buckets at risk?

Catalogued multiple security vulnerabilities across S3 buckets >

Yes, you have a significant number of S3 bucket issues — **123 failed findings** across your AWS account (`552455647653`). Here's a breakdown:

🔴 Critical — Public Access (2 findings)

These buckets are **publicly accessible** via bucket policy, which is the highest-risk issue:

Bucket	Region	Note
`prowler-cfn-templates-example`	eu-west-1	
`demo-bucket-1763841210`	us-east-1	🆕 New

🟠 High — Cross-Account Access & Account Config (4 findings)

Bucket / Resource	Issue
`prowler-cfn-templates-example`	Cross-account access allowed
`prowler-reports-demo`	Cross-account access allowed
`demo-bucket-1763841210`	Cross-account access allowed 🆕
Account 552455647653	**Block Public Access not configured at account level**

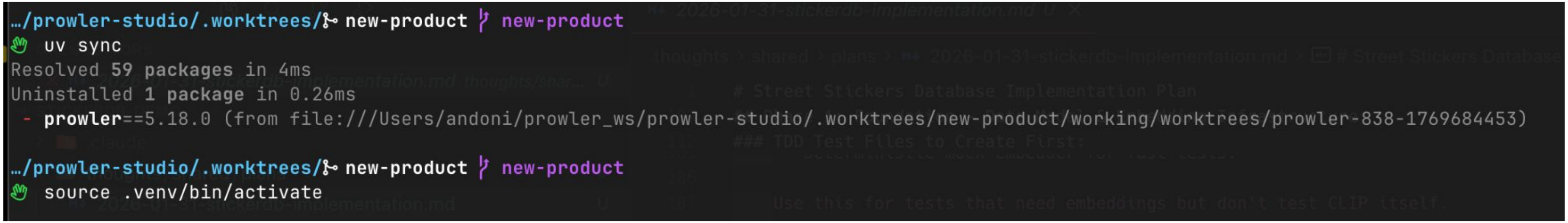
🟡 Medium — Widespread misconfigurations

Across ~13 buckets, recurring issues include:

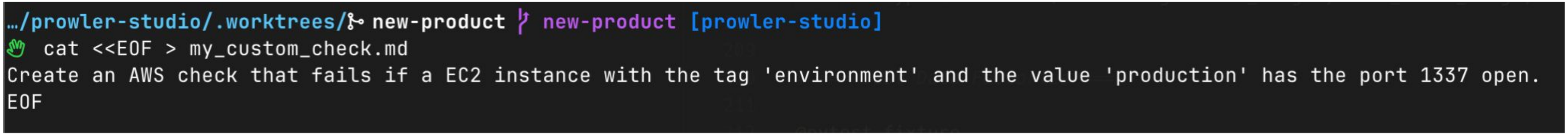
- **Server access logging disabled** — on all b ets (13 findings)
- **Insecure transport allowed (no HTTPS enforcement)** — on all buckets (13 findings)

prowler-studio

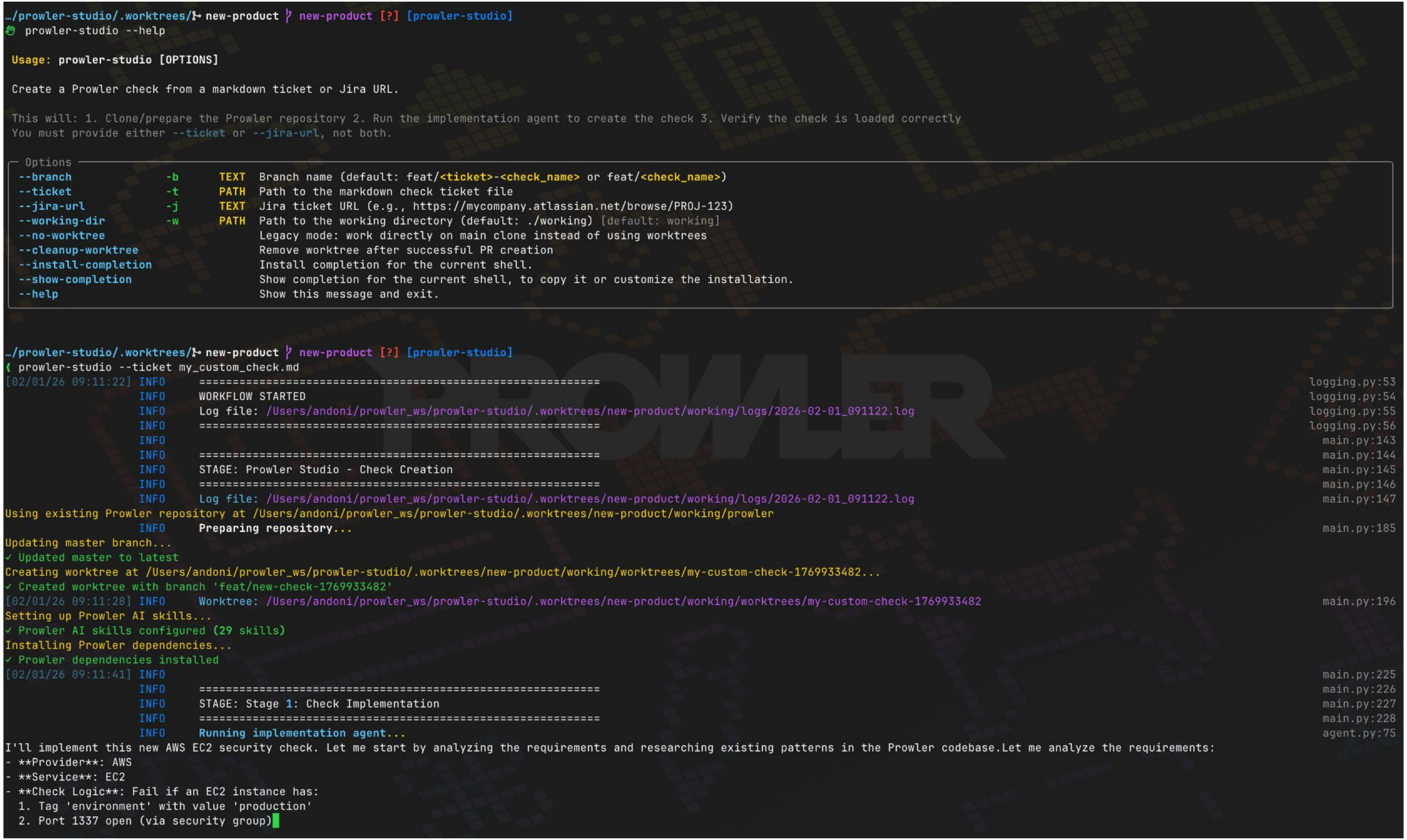
https://github.com/prowler-cloud/prowler-studio/tree/new-product



```
…/prowler-studio/.worktrees/ new-product  new-product
✋ uv sync
Resolved 59 packages in 4ms
Uninstalled 1 package in 0.26ms
 - prowler==5.18.0 (from file:///Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/worktrees/prowler-838-1769684453)

…/prowler-studio/.worktrees/ new-product  new-product
✋ source .venv/bin/activate
```



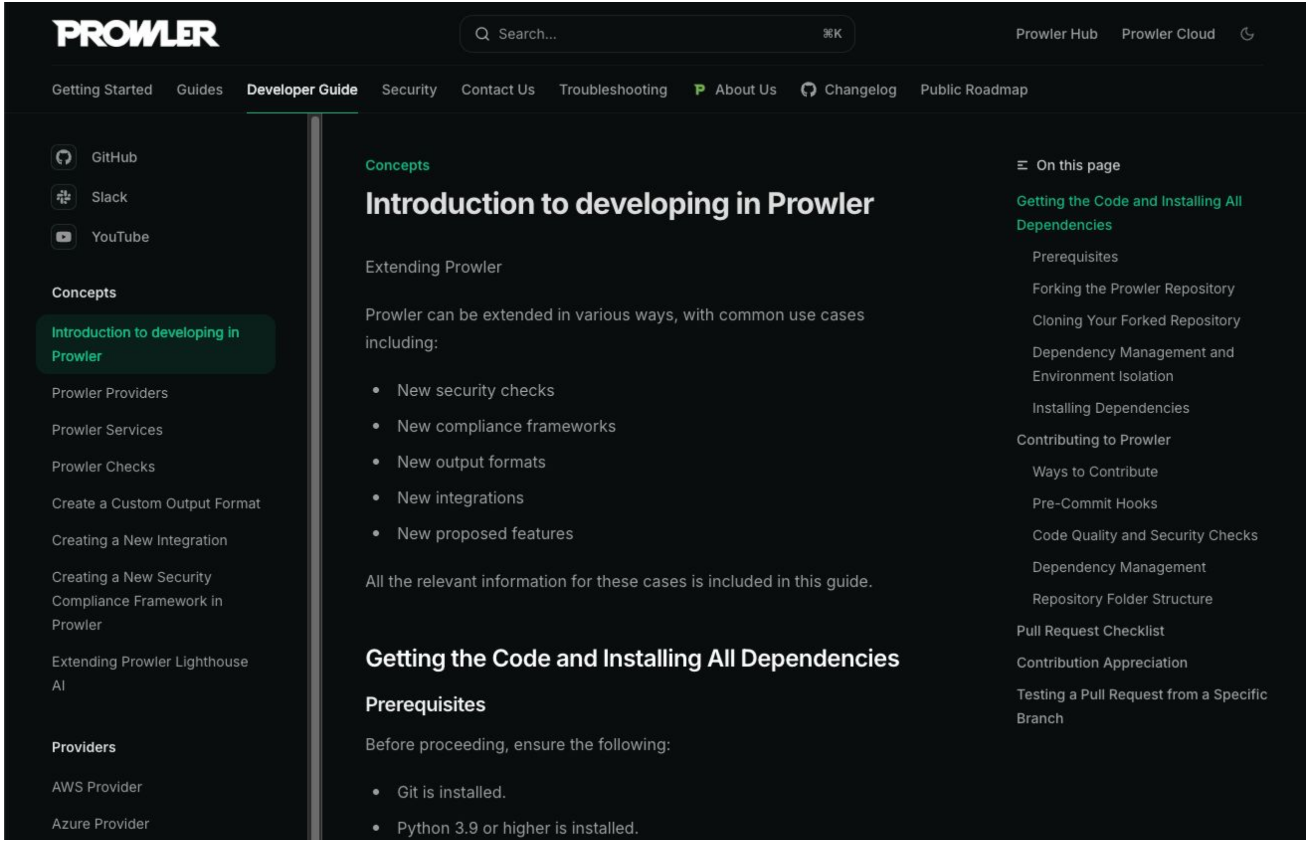
```
…/prowler-studio/.worktrees/ new-product  new-product [prowler-studio]
✋ cat <<EOF > my_custom_check.md
Create an AWS check that fails if a EC2 instance with the tag 'environment' and the value 'production' has the port 1337 open.
EOF
```



```
…/prowler-studio/.worktrees/ new-product  new-product [?] [prowler-studio]
  prowler-studio --help

 Usage: prowler-studio [OPTIONS]

 Create a Prowler check from a markdown ticket or Jira URL.

 This will: 1. Clone/prepare the Prowler repository 2. Run the implementation agent to create the check 3. Verify the check is loaded correctly
 You must provide either --ticket or --jira-url, not both.

╭─ Options ────────────────────────────────────────────────────────────────────────────────────────────────────────────────────╮
│ --branch              -b      TEXT  Branch name (default: feat/<ticket>-<check_name> or feat/<check_name>)                   │
│ --ticket              -t      PATH  Path to the markdown check ticket file                                                   │
│ --jira-url            -j      TEXT  Jira ticket URL (e.g., https://mycompany.atlassian.net/browse/PROJ-123)                  │
│ --working-dir         -w      PATH  Path to the working directory (default: ./working) [default: working]                    │
│ --no-worktree                       Legacy mode: work directly on main clone instead of using worktrees                      │
│ --cleanup-worktree                  Remove worktree after successful PR creation                                             │
│ --install-completion                Install completion for the current shell.                                                │
│ --show-completion                   Show completion for the current shell, to copy it or customize the installation.         │
│ --help                              Show this message and exit.                                                              │
╰──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────╯


…/prowler-studio/.worktrees/ new-product  new-product [?] [prowler-studio]
( prowler-studio --ticket my_custom_check.md
[02/01/26 09:11:22] INFO     ============================================================                              logging.py:53
                    INFO     WORKFLOW STARTED                                                                          logging.py:54
                    INFO     Log file: /Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/logs/2026-02-01_091122.log   logging.py:55
                    INFO     ============================================================                              logging.py:56
                    INFO                                                                                                  main.py:143
                    INFO     ============================================================                                 main.py:144
                    INFO     STAGE: Prowler Studio - Check Creation                                                       main.py:145
                    INFO     ============================================================                                 main.py:146
                    INFO     Log file: /Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/logs/2026-02-01_091122.log   main.py:147
Using existing Prowler repository at /Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/prowler
                    INFO     Preparing repository...                                                                      main.py:185
Updating master branch...
✓ Updated master to latest
Creating worktree at /Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/worktrees/my-custom-check-1769933482...
✓ Created worktree with branch 'feat/new-check-1769933482'
[02/01/26 09:11:28] INFO     Worktree: /Users/andoni/prowler_ws/prowler-studio/.worktrees/new-product/working/worktrees/my-custom-check-1769933482   main.py:196
Setting up Prowler AI skills...
✓ Prowler AI skills configured (29 skills)
Installing Prowler dependencies...
✓ Prowler dependencies installed
[02/01/26 09:11:41] INFO                                                                                                  main.py:225
                    INFO     ============================================================                                 main.py:226
                    INFO     STAGE: Stage 1: Check Implementation                                                         main.py:227
                    INFO     ============================================================                                 main.py:228
                    INFO     Running implementation agent...                                                              agent.py:75
I'll implement this new AWS EC2 security check. Let me start by analyzing the requirements and researching existing patterns in the Prowler codebase.Let me analyze the requirements:
- **Provider**: AWS
- **Service**: EC2
- **Check Logic**: Fail if an EC2 instance has:
  1. Tag 'environment' with value 'production'
  2. Port 1337 open (via security group)
```

IT'S
DEMO TIME

How to contribute?


PROWLER
Search...
⌘K
Prowler Hub
Prowler Cloud
Getting Started
Guides
Developer Guide
Security
Contact Us
Troubleshooting
About Us
Changelog
Public Roadmap
GitHub
Slack
YouTube
Concepts
Introduction to developing in Prowler
Prowler Providers
Prowler Services
Prowler Checks
Create a Custom Output Format
Creating a New Integration
Creating a New Security Compliance Framework in Prowler
Extending Prowler Lighthouse AI
Providers
AWS Provider
Azure Provider
On this page
Getting the Code and Installing All Dependencies
Prerequisites
Forking the Prowler Repository
Cloning Your Forked Repository
Dependency Management and Environment Isolation
Installing Dependencies
Contributing to Prowler
Ways to Contribute
Pre-Commit Hooks
Code Quality and Security Checks
Dependency Management
Repository Folder Structure
Pull Request Checklist
Contribution Appreciation
Testing a Pull Request from a Specific Branch

Concepts

Introduction to developing in Prowler

Extending Prowler

Prowler can be extended in various ways, with common use cases including:

- New security checks
- New compliance frameworks
- New output formats
- New integrations
- New proposed features

All the relevant information for these cases is included in this guide.

Getting the Code and Installing All Dependencies

Prerequisites

Before proceeding, ensure the following:

- Git is installed.
- Python 3.9 or higher is installed.

goto.prowler.com/devguide

How to Create a new Check - I

- Prowler contains a providers folder which has a folder per provider:

```
prowler/providers/<provider>
     |
     |- aws
     |- azure
     |- gcp
     |- kubernetes
     |- common # common functions and libraries for all providers
```

- Inside the provider folder there is a `<provider>_provider.py` where the credentials are managed and the session is generated so Prowler can start the scan for the specified provider.

```
prowler/providers/aws
     |
     |- aws_provider.py
     |- __init__.py # empty init file to treat the folder as a package
     |- lib # necessary libraries for provider
     |- services
     |- ...
```

How to Create a new Check - II

- For each provider, there is a folder per service, e.g.:
  - `prowler/providers/aws/services/`

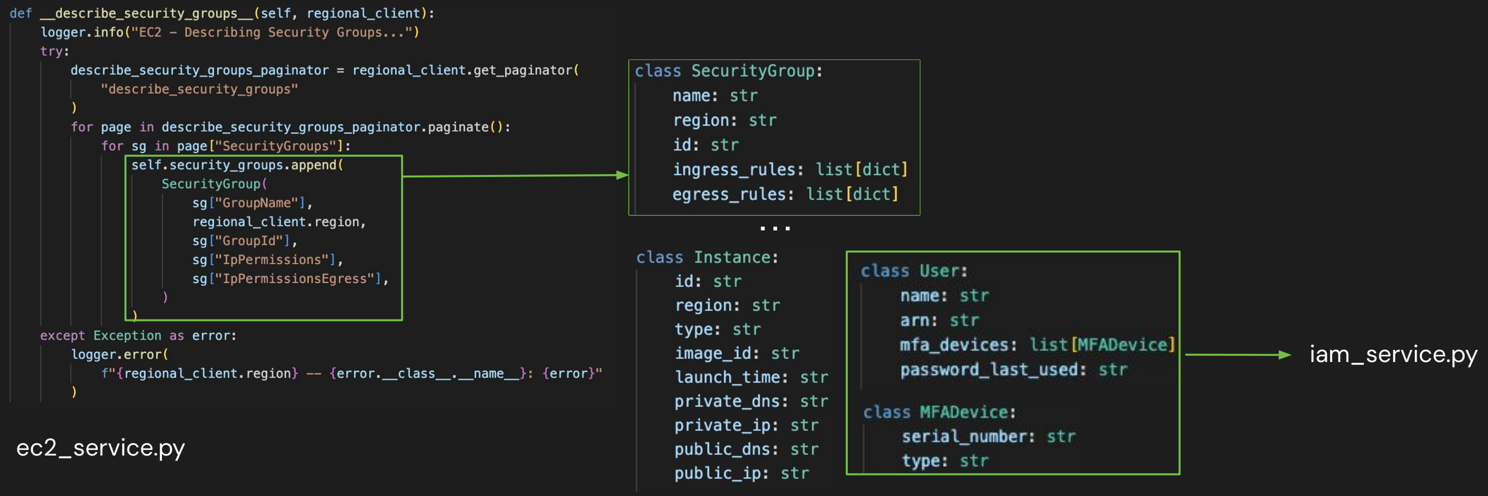
```
     |
     |- iam
          |- iam_client.py # Initialise IAM Service
          |- iam_service.py # Gather IAM Information with provider SDK
          |- __init__.py
     |- ec2
          |- ec2_client.py # Initialise EC2 Service
          |- ec2_service.py # Gather EC2 Information with provider SDK
          |- __init__.py
     |- ...
```

How to Create a new Check - III

- Service information is gathered with the API Calls from the provider SDK (e.g., Boto3).
    - This information is then parsed inside every check.
    - In AWS, API calls are parallelized by region to increase performance by generating a client per AWS Service and Region.

How to Create a new Check - IV

- Each Service has a class per type of resource:
    - Attributes filled by the API calls.
    - E.g. IAM User, EC2 Instance or Security Group…



```python
def __describe_security_groups__(self, regional_client):
    logger.info("EC2 - Describing Security Groups...")
    try:
        describe_security_groups_paginator = regional_client.get_paginator(
            "describe_security_groups"
        )
        for page in describe_security_groups_paginator.paginate():
            for sg in page["SecurityGroups"]:
                self.security_groups.append(
                    SecurityGroup(
                        sg["GroupName"],
                        regional_client.region,
                        sg["GroupId"],
                        sg["IpPermissions"],
                        sg["IpPermissionsEgress"],
                    )
                )
    except Exception as error:
        logger.error(
            f"{regional_client.region} -- {error.__class__.__name__}: {error}"
        )
```

ec2_service.py

```python
class SecurityGroup:
    name: str
    region: str
    id: str
    ingress_rules: list[dict]
    egress_rules: list[dict]
```

...

```python
class Instance:
    id: str
    region: str
    type: str
    image_id: str
    launch_time: str
    private_dns: str
    private_ip: str
    public_dns: str
    public_ip: str
```

```python
class User:
    name: str
    arn: str
    mfa_devices: list[MFADevice]
    password_last_used: str

class MFADevice:
    serial_number: str
    type: str
```

iam_service.py

How to Create a new Check - V

- Inside each service folder there is a folder per check:

```
prowler/providers/<provider>/services/<service>/<check_id>/
```

- The ID of the check must follow the pattern:

```
service_subservice_action → ec2_ami_public
```

- The files inside the check folder are:

```
prowler/providers/<provider>/services/<service>/<check_id>/
    |
    |- <check_id>.metadata.json # contains the check’s metadata
    |- <check_id>.py # contains the check’s logic
    |- __init__.py # empty init file to treat the folder as a package
    |
```

Check’s Metadata

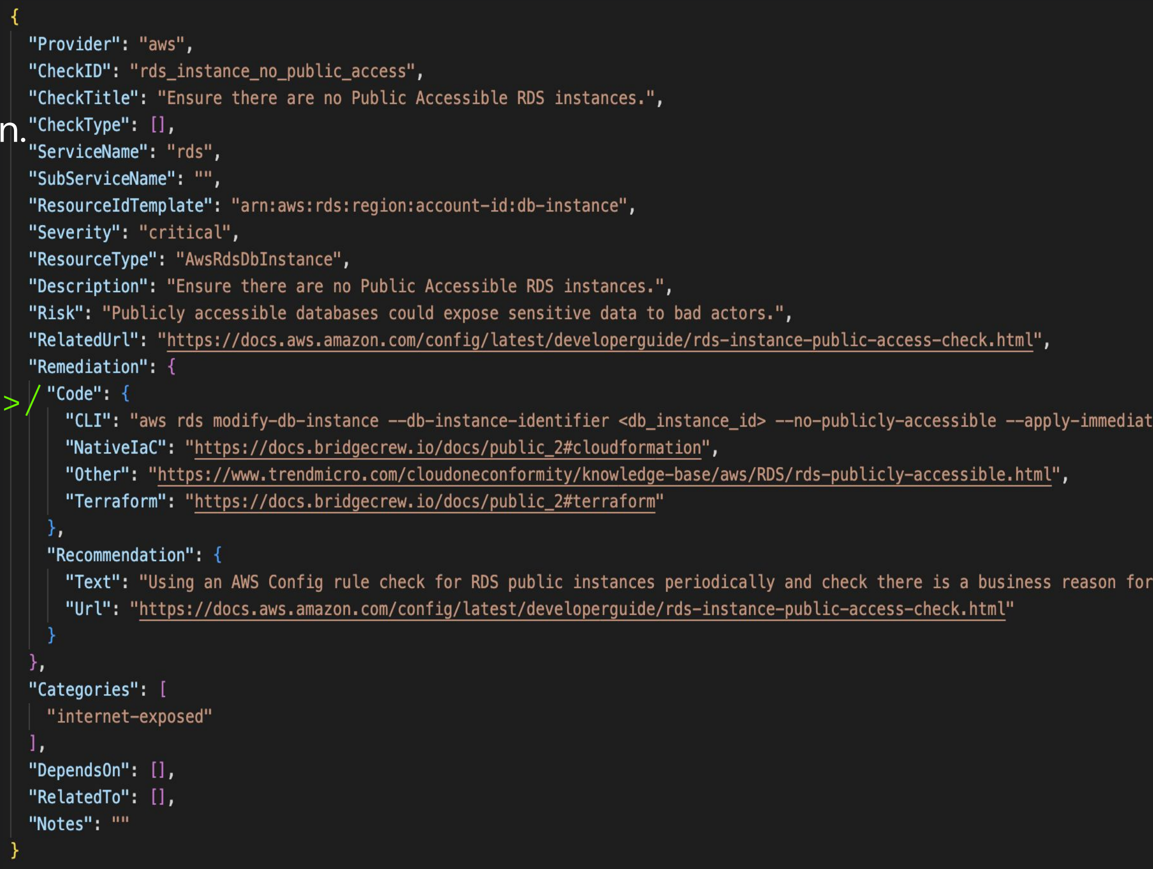
- JSON file containing check information.
- Necessary for check execution.

  `<check_id>.metadata.json`

- Inside folder

  `providers/<provider>/<service>/<check-id>/`

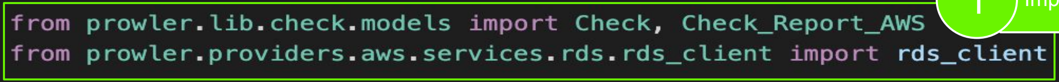
rds_instance_no_public_access.metadata.json



```json
{
  "Provider": "aws",
  "CheckID": "rds_instance_no_public_access",
  "CheckTitle": "Ensure there are no Public Accessible RDS instances.",
  "CheckType": [],
  "ServiceName": "rds",
  "SubServiceName": "",
  "ResourceIdTemplate": "arn:aws:rds:region:account-id:db-instance",
  "Severity": "critical",
  "ResourceType": "AwsRdsDbInstance",
  "Description": "Ensure there are no Public Accessible RDS instances.",
  "Risk": "Publicly accessible databases could expose sensitive data to bad actors.",
  "RelatedUrl": "https://docs.aws.amazon.com/config/latest/developerguide/rds-instance-public-access-check.html",
  "Remediation": {
    "Code": {
      "CLI": "aws rds modify-db-instance --db-instance-identifier <db_instance_id> --no-publicly-accessible --apply-immediat
      "NativeIaC": "https://docs.bridgecrew.io/docs/public_2#cloudformation",
      "Other": "https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/RDS/rds-publicly-accessible.html",
      "Terraform": "https://docs.bridgecrew.io/docs/public_2#terraform"
    },
    "Recommendation": {
      "Text": "Using an AWS Config rule check for RDS public instances periodically and check there is a business reason for
      "Url": "https://docs.aws.amazon.com/config/latest/developerguide/rds-instance-public-access-check.html"
    }
  },
  "Categories": [
    "internet-exposed"
  ],
  "DependsOn": [],
  "RelatedTo": [],
  "Notes": ""
}
```

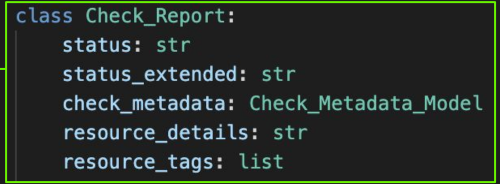
Check's Logic

- Each check must generate a report per finding.



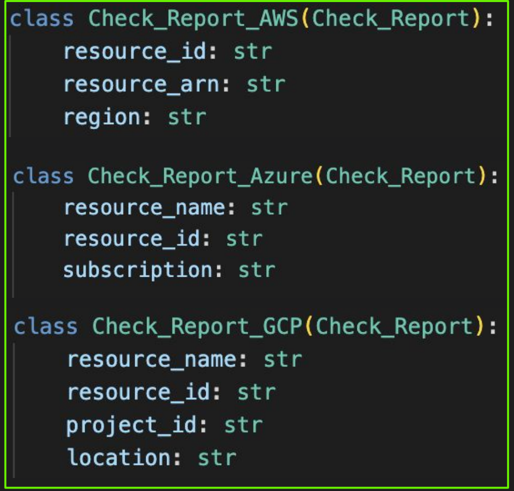
```
from prowler.lib.check.models import Check, Check_Report_AWS
from prowler.providers.aws.services.rds.rds_client import rds_client
```

1 Import classes and service client.

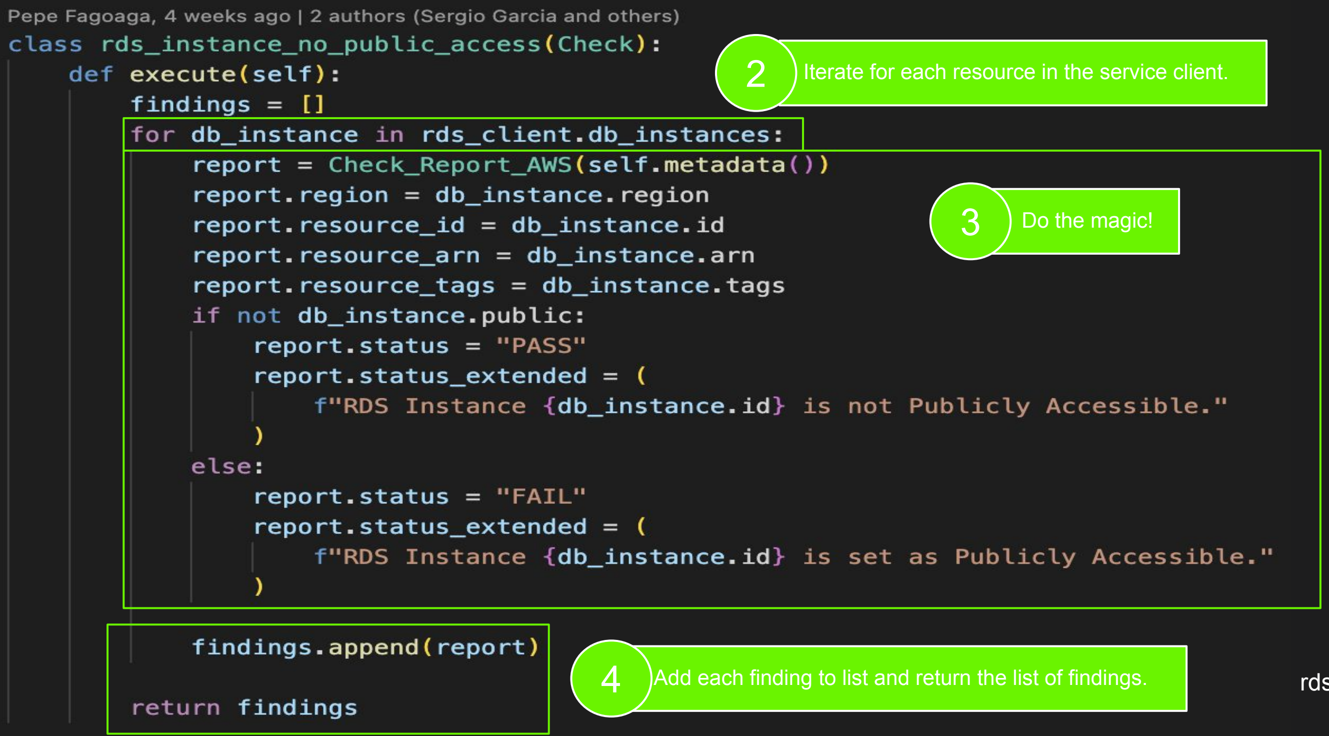


```
class Check_Report:
    status: str
    status_extended: str
    check_metadata: Check_Metadata_Model
    resource_details: str
    resource_tags: list
```

+



```
class Check_Report_AWS(Check_Report):
    resource_id: str
    resource_arn: str
    region: str

class Check_Report_Azure(Check_Report):
    resource_name: str
    resource_id: str
    subscription: str

class Check_Report_GCP(Check_Report):
    resource_name: str
    resource_id: str
    project_id: str
    location: str
```



```
Pepe Fagoaga, 4 weeks ago | 2 authors (Sergio Garcia and others)
class rds_instance_no_public_access(Check):
    def execute(self):
        findings = []
        for db_instance in rds_client.db_instances:
            report = Check_Report_AWS(self.metadata())
            report.region = db_instance.region
            report.resource_id = db_instance.id
            report.resource_arn = db_instance.arn
            report.resource_tags = db_instance.tags
            if not db_instance.public:
                report.status = "PASS"
                report.status_extended = (
                    f"RDS Instance {db_instance.id} is not Publicly Accessible."
                )
            else:
                report.status = "FAIL"
                report.status_extended = (
                    f"RDS Instance {db_instance.id} is set as Publicly Accessible."
                )

            findings.append(report)

        return findings
```

2 Iterate for each resource in the service client.

3 Do the magic!

4 Add each finding to list and return the list of findings.

rds_instance_no_public_access.py

How to Create a Compliance Framework

- Create a compliance file in the specific provider folder, e.g, `prowler/compliance/<provider>/`
- Name as the following pattern: `<framework>_<version>_<provider>.json`
- Create the compliance framework data model in `prowler/lib/outputs/models.py`
- Optional: Create the CLI table output in `prowler/lib/outputs/compliance.py`
- Test it with:

```
./prowler-cli.py <provider> --compliance <framework>_<version>_<provider>
```

CIS-x.x framework for a provider

1. Create compliance file with the framework name inside `providers/compliance/<provider>`
   - *E.g.*: `cis_1.5_workshop_aws.json`
2. Fill the compliance framework information in the JSON:
   - Framework, Version, Provider and Description
3. Add the CIS-X.X requirements with:
   - Requirement ID and Description
   - Requirement Attributes
   - List of Prowler checks that cover the requirement
4. Run it with:

```
./prowler-cli.py aws --compliance cis_1.5_workshop_aws
```

❓ HINT: If you get stuck, check the compliance for the chosen provider inside this folder: https://github.com/prowler-cloud/prowler/blob/master/prowler/compliance/