Managed external secrets partner onboarding guide

AWS Secrets Manager

AWS Secrets Manager: Managed external secrets partner onboarding guide

Table of Contents

Secrets Manager managed external secrets partner onboarding guide

This guide provides the information you need to become a partner with AWS Secrets Manager managed external secrets. When you integrate with managed external secrets, your customers can securely manage their credentials through AWS.

Why integrate with Secrets Manager

When you integrate with Secrets Manager, your customers get the following advantages:

- **Unified third-party secret management** – Secrets Manager provides a standardized, predefined format for storing your software secrets to streamline the management of credentials. This approach reduces the complexity and overhead of custom credential management strategies for your customers.
- **Managed rotation** – Secrets Manager handles the credential rotation process by default. This provides automatic, compliance-driven secret rotation with no operational overhead. Customers no longer need to create custom Lambda functions or manual processes.
- **Seamless integration** – Native partner integrations provide visibility and transparent lifecycle management for all of your secrets. You get:
  - Comprehensive security controls managed with AWS Identity and Access Management permissions.
  - Automated workflows that reduce manual intervention and human error.
  - Flexibility to manage secrets across AWS and other environments.
  - Transparent secret management workflows for visibility and compliance.

Terminology

The following terms are used throughout this guide to describe managed external secrets concepts and the onboarding process.

Secrets

Secrets refer to sensitive credentials, API keys, OAuth tokens, and configuration data used by third-party software applications that integrate with AWS services. These secrets are critical for

secure authentication and communication between systems, and require careful management to prevent unauthorized access.

AWS Secrets Manager

A secure service for centrally managing and retrieving credentials and other secrets.

Managed external secrets

A specialized secret type in Secrets Manager for third-party software credentials.

Third-party software vendor

Third-party companies that develop and sell software products compatible with AWS.

AWS Partner Network (APN)

A global AWS program providing support to software vendors and service providers.

Secret rotation

Automated process of periodically updating secret values to enhance security.

Rotation configuration

Technical specifications defining how secret rotation is done.

Rotation schedule

How often secrets are automatically rotated.

Single user rotation

A rotation method that updates credentials for one secret for one user at a time.

Alternating users rotations

A rotation method that maintains two sets of active credentials for zero downtime updates. The rotation process rotates one secret, the application can rely on the other secret to avoid disruption.

Service endpoint

The specific URL where third-party software accepts API calls for secret management.

JSON format

The format used to define secret structures.

How to onboard with managed external secrets

To onboard your secrets, you must:

1. Evaluate your use case with the AWS Secrets Manager team.
2. Submit the required details.
3. Roll out your integration to the public.

In addition, you must monitor how your customers use managed external secrets and support them if there are any production issues. The following sections provide the details.

Step 1: Discuss your integration with Secrets Manager

Duration: approximately one week

To begin the onboarding process, engage with the Secrets Manager team to discuss your specific use case. This step ensures a smooth integration and addresses any questions you have.

Contact information

- **Email:** aws-secrets-mgr-partner-onboarding@amazon.com
- **Alternative:** If you have an existing relationship with an AWS technical account manager (TAM) or other AWS contact, you may reach out to them directly.

What to include in your enquiry:

- A detailed description of your use case.
- Any questions or concerns about the integration process.
- Your organization's security policies and compliance requirements (if applicable).

The initial evaluation helps the Secrets Manager team understand your needs and provide individual guidance for a successful onboarding experience.

Step 2: Provide integration specifications

Duration: Typically one to two weeks.

After reaching alignment with the Secrets Manager team, you need to provide the following details to begin the onboarding process. These include essential details about your service along with technical details.

The Secrets Manager team reviews these details. After they are confirmed, the team onboards you as an integration partner.

You must provide all of the information to begin.

Prerequisite

You must be a member of the AWS Partner Network. For more information about the benefits of being a member, see Join the AWS Partner Network.

Share the following details with the Secrets Manager team:

- Your AWS Partner Network ID.
- The name of your service.
- A 50-word or less description of the use case for your secret.
- A 50-word summary of your secret type to help customers identify the secret that they are generating. If your service supports more than one secret type, each must be onboarded separately.
- The format of your secret. Secrets Manager uses the format to validate that customer provided secret metadata complies with your specific format. For example:

```
{
  "consumerKey":"<client ID>",
  "consumerSecret":"<client secret>",
  "baseUri":"https://<domain>.my.example.com",
  "appId":"<app ID>",
  "consumerId":"<consumer ID>"
}
```

- The defined rotation strategy for your secret. Your customer can choose from the supported rotation strategies when creating secrets.
  - Single user rotation
  - Alternating users rotation (requires support for multiple active users)
- The rotation configuration that Secrets Manager uses to run the rotation workflow. Typical configuration parameters are:

- Sample Java code that has your specific rotation workflow logic to rotate the secret and update Secrets Manager.
- The specific URL of the service endpoint that Secrets Manager invokes as part of the rotation workflow. Include availability and response time requirements. Also include Region-specific URLs if applicable.
- Authentication mechanisms for AWS to access the URL.
- The rotation schedule that customers can define for their secrets. This value is used as a default if the customer doesn't specify a value. Choose one of the following: 4 hrs | 7 days | 30 days.

- Help text and placeholder text for customer visible fields.
- Any additional service-specific details or requirements.

Submit the information to the following email address:

- aws-secrets-mgr-partner-onboarding@amazon.com

With the subject line:

- [Third-party software vendor name] partner onboarding request

Step 3: Launch your integration

Secrets Manager conducts joint testing with you prior to the launch. Based on the test results and receiving alignment with you, we will launch the integration. Secrets Manager sends an official communication with details about your new offering. AWS may send a launch announcement to its customers.

Support

After the integration launches, customers can use managed external secrets to secure credentials for your service. The AWS Secrets Manager team is the first point of contact for troubleshooting customer issues. We contact your team for additional support in the troubleshooting process.

For high severity issues, we expect a response within 24 hours, and resolutions should not take an unreasonable amount of time.

To facilitate this process, provide your contact details and your expected service level agreement (SLA) for high-severity issues. This helps us ensure that we can collaborate effectively to resolve issues in a timely manner.

If you have any specific requirements or preferences for communication channels, let us know.

Document History for AWS Secrets Manager managed external secrets onboarding guide

The following table describes the important changes to the documentation since the last release of Secrets Manager managed external secrets. In addition to the important changes listed here, we also update the documentation frequently to improve the descriptions and examples, and to address the feedback that you send to us. To be notified about important changes, subscribe to the RSS feed.

Change	Description	Date
Initial release	This is the initial release of the Secrets Manager managed external secrets onboarding guide.	October 18, 2025