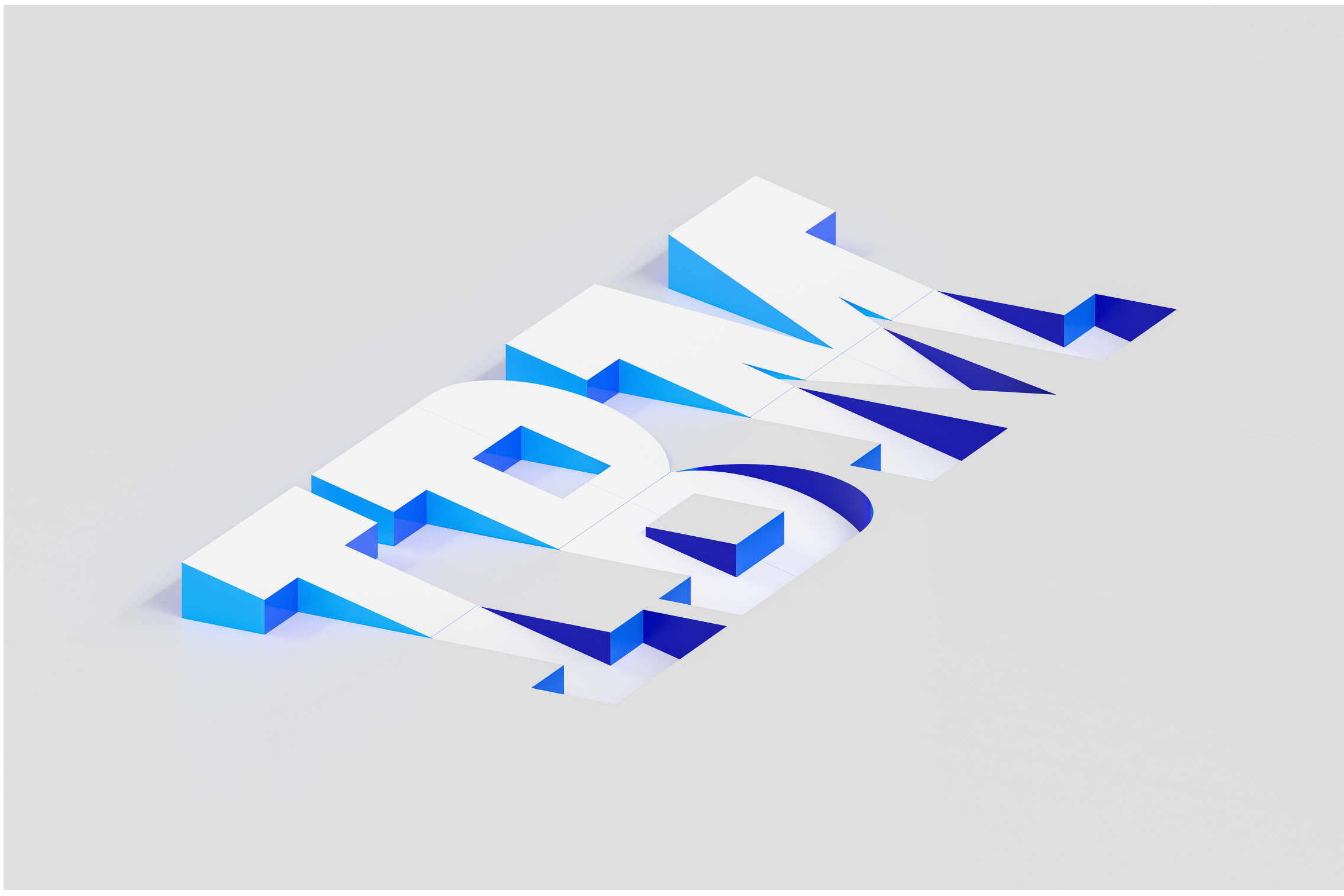
IBM Cloud

Security and Compliance Center

Product guide



IBM

Evaluate your Watson Machine Learning resources for security and compliance

⚠ **Important:** Effective 15 Dec 2025, Security and Compliance Center is end of support. Any existing service instances on that date will be non-functional. Start your transition now to Security and Compliance Center Workload Protection, which is readily available and offers advanced cloud security posture management (CSPM). For more see, see Transitioning to Security and Compliance Center Workload Protection .

As the focal in charge of setting up the compliance posture in an environment that contains your SaaS services, such as Watson Machine Learning, you can use IBM Cloud® Security and Compliance Center. This tutorial walks you through scanning your Watson Machine Learning resources against the AI Security Guardrails 2.0 profile.

To scan the Watson Machine Learning resources in your account, you use an IAM API key that you store in Secrets Manager as an IAM credentials or arbitrary secret. After you create a target, you can then add the API key of an IAM service ID that is part of the IBM watsonx project.

Before you begin

Before you get started, complete the following tasks.

- Make sure that you can create IAM credentials for your organization.
- Create an instance of Secrets Manager, if you don't have an existing one.

Step 1: Configure the required access permissions for Security and Compliance Center

Before you can scan your watson resources, you must set up the required access permissions.

Create service credentials

First, create a service ID and API key that you can later store in your Secrets Manager instance.

- Create a service ID with `Viewer` role to access your Watson Machine Learning service. Go to **Manage** > **Access (IAM)** > **Service ID**.
- Create an API key from that service ID to access the account that contains your Watson Machine Learning service. Go to **Manage** > **Access (IAM)** > **API keys**.

Authorize Secrets Manager to connect to Security and Compliance Center

Before you can scan your Watson Machine Learning resources, connect your instance of Security and Compliance Center and Secrets Manager.

Create an authorization between your Security and Compliance Center instance and your Secrets Manager instance.

1. Go to **Manage** > **Access (IAM)** > **Authorizations**.
2. Create an authorization with the following values.
    a. In the **Source** section, add the account ID of the account that contains the Security and Compliance Center instance as the **Source account**.
    b. Select Security and Compliance Center as the **Service**.
    c. In the **Resources** field, add the service instance ID.
    d. In the **Target** section, select Secrets Manager as the **Service**.
    e. Add the instance ID in the **Resources** field.
    f. Assign `SecretsReader` as the **Role**.

Create a trusted profile

To scan your account, create a trusted profile with the following access policies and assign the specified roles.

- All Account Management services (`Viewer` , `Service Configuration Reader`)
- Kubernetes Service (`Reader` , `Viewer` , `Administrator` , `Service Configuration Reader`)
- All Identity and Access enabled services (`Reader` , `Viewer` , `Service Configuration Reader`)

Step 2: Store your service credentials in Secrets Manager

Next, it's time to store the API key in Secrets Manager so that Security and Compliance Center can access it to scan your Watson Machine Learning resources.

In your instance of Secrets Manager, create an arbitrary or IAM credentials secret to store the API key that you previously created.

If you are using an arbitrary secret, save the API key as the secret value. If you choose to use an IAM credentials secret, use the service ID that is associated with the API key that you created.

> ⚠ **Important:** The secret must remain unlocked for Security and Compliance Center to be able to access and read it.

Step 3: Create a target

Now that your Security and Compliance Center and Secrets Manager instances are connected, you can target the trusted profile that you created.

1. Navigate to your Security and Compliance Center instance.
2. Go to **Settings**.
3. In the **Targets** section, click **Add**.
4. In the **Add target** page, enter the **Name**, **Account ID**, and **Trusted profile ID** of your target account.
5. Click **Add**.

Step 4: Assign credentials to scan Watson Machine Learning

After you create a target, you can assign the API key to the Watson Machine Learning resources that you want to scan.

1. In the **What's next** section, click **Assign credentials** to assign credentials that you want to use when you're scanning your Watson Machine Learning resources.
2. In the **Select credential** tab, you can assign the secret that contains the API key.
3. Select the **Secrets Manager instance**, **Secret group**, and **Secret type**.
4. Select the secret that contains the API key, then click **Next**.
5. Click **Add** icon (+) to select the Watson Machine Learning instances in your target account that you want to access with this credential. You can assign this credential to all or specific instances of the service.
6. Click **Assign**.

> ☑ **Tip:** Alternatively, you can select **Locate by CRN** to enter the CRN of the secret that you want to use directly.

Step 5: Create a scope

A scope is the grouping of resources that you want to evaluate. For help with creating a scope, see Targeting your resources.

Step 6: Scan your resources

After you assign the credentials, you're free to start scanning your Watson Machine Learning resources. Complete the following steps to do so.

1. In the **Profiles** section of the console, select **AI Security Guardrails 2.0**. A details page opens.
2. In the **Attachments** tab, click **Create**.
3. Target your resources by selecting a **Scope**. Optionally, you can choose to exclude portions of your selected scope to ensure that they are not included in your scan.
4. Click **Next**.
5. Unless your profile contains additional controls, you can skip the **Parameters** tab by clicking **Next**.
6. Toggle **Enable scan** to **On** to ensure that the scan runs.
7. Select the frequency at which you want to evaluate your resource. Options include **Every day**, **Every 7 days**, and **Every 30 days**.
8. Optionally, you can enable notifications.
9. Click **Next**. Review your selections and click **Create**.

Next steps

Now that you finished evaluating your Watson Machine Learning resources against the AI Security Guardrails 2.0 profile, you can view detailed results in the dashboard and download a report.