Getting Started with AI Defense

To begin using AI Defense, follow these initial steps to activate and configure your subscription:

1. Log into Security Provisioning and Administration page.
2. At the top left of the window, click the **Enterprise chooser** and pick your enterprise name.
3. Go to the **Overview** tab and click **Claim Subscription** at the upper right. Paste your subscription claim code, click **Next**, choose your region, and finish the subscription wizard.
4. In a new browser tab, open the AI Defense page.

Add Users

To add more users to the private preview edition of AI Defense, contact your Cisco support team.

Initial Configuration for Key Use Cases

Below, we list the most common AI security use cases and provide links for setting up AI Defense to handle each case.

Discover AI Assets within cloud accounts

Connect AI Defense to your Multicloud Defense (MCD) tenant and connect MCD to your cloud account as explained in Initial Configuration of AI Assets.

Note AWS is supported for early access.

Discover third-party models being called from within cloud accounts

Connect AI Defense to your Multicloud Defense (MCD) tenant and connect MCD to your cloud account as explained in Initial Configuration of AI Assets.

Note AWS is supported for early access.

Perform Vulnerability Scans for AI Assets

Vulnerability Scans for models in cloud accounts

Prerequisite: You must have a Multicloud Defense tenant that's connected to AI Defense and connected to your cloud account. To set this up, see Initial Configuration of AI Assets.

To set up for vulnerability scans: Connect your cloud account to AI Defense as shown in Initial Configuration of AI Validation.

To run a vulnerability scan: Navigate to AI Assets and click the Validate button to validate the desired model.

Note AWS is supported for early access.

Vulnerability Scans for all other applications and models

Manually register an application and perform the validation as explained in Finding an Asset on the AI Validation page

Provide runtime protection for LLM prompts and responses

Runtime protection for third-party LLM applications

Available early 2025.

Runtime protection for private cloud-based LLM applications and models

Available early 2025.

Runtime protections for other applications and models

1. Step 1: Register and connect an application as shown in Applications.
2. Step 2: Create and assign a policy as shown in Policies.

Discover third-party AI applications

Connect AI Defense to your Cisco Secure Access tenant as explained in Initial Configuration of AI Application Discovery.