

Implementing Automation for Cisco Security Solutions (SAUI) v1.0

What you'll learn in this course

The **Implementing Automation for Cisco Security Solutions (SAUI) v1.0** course teaches you how to design advanced automated security solutions for your network. Through a combination of lessons and hands-on labs, you will master the use of modern programming concepts, RESTful Application Program Interfaces (APIs), data models, protocols, firewalls, web, Domain Name System (DNS), cloud, email security, and Cisco® Identity Services Engine (ISE) to strengthen cybersecurity for your web services, network, and devices. You will learn to work within the following platforms: Cisco Firepower® Management Center, Cisco Firepower Threat Defense, Cisco ISE, Cisco pxGrid, Cisco Stealthwatch® Enterprise, Cisco Stealthwatch Cloud, Cisco Umbrella®, Cisco Advanced Malware Protection (AMP), Cisco Threat grid, and Cisco Security Management Appliances. This course will teach you when to use the API for each Cisco security solution to drive network efficiency and reduce complexity.

This course prepares you for **300-735 Automating and Programming Cisco Security Solutions (SAUTO)** certification exam. **Introducing Automation for Cisco Solutions (CSAU)** is required prior to enrolling in **Implementing Automation for Cisco Security Solutions (SAUI)** because it provides crucial foundational knowledge essential to success.

Course duration

- Instructor-led training: 3 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 3 days of web-based classes with hands-on lab practice
- E-learning: Equivalent to 3 days in the classroom

How you'll benefit

This course will help you:

- Gain the knowledge and skills to use automation and programmability to design more efficient networks, increase scalability, and protect against cyberattacks
- Learn how to create APIs to streamline cloud-based, network security solutions for your organization
- Prepares you for the **300-735 SAUTO** exam



What to expect in the exam

The **300-735 SAUTO** exam certifies your knowledge and skills for implementing Security automated solutions including programming concepts, RESTful APIs, data models, protocols, firewalls, web, DNS, cloud, email security, and ISE.

After you pass **300-735 SAUTO** exam, you earn the **Cisco Certified DevNet Specialist - Security Automation and Programmability** certification, and you satisfy the concentration exam requirement for these professional-level certifications:

- [CCNP® Security](#)
- [Cisco Certified DevNet Professional](#)

Who should enroll

This course is designed primarily for professionals in job roles such as:

- Network engineer
- Systems engineer
- Wireless engineer
- Consulting systems engineer
- Technical solutions architect
- Network administrator
- Wireless design engineer
- Network manager
- Sales engineer
- Account manager

How to enroll

- For instructor-led training, visit the [Cisco Learning Locator](#).
- For private group training, visit [Cisco Private Group Training](#).
- For e-learning, visit the [Cisco Learning Network Store](#).
- For digital library access, visit [Cisco Learning Library](#).
- For other ways to purchase e-learning, contact us at: learning-bdm@cisco.com.

Technology areas

- Network automation
- Security



Course details

Objectives

After taking this course, you should be able to:

- Describe the overall architecture of the Cisco security solutions and how APIs help enable security
- Know how to use Cisco Firepower APIs
- Explain how pxGrid APIs function and their benefits
- Demonstrate what capabilities the Cisco Stealthwatch APIs offer and construct API requests to them for configuration changes and auditing purposes
- Describe the features and benefits of using Cisco Stealthwatch Cloud APIs
- Learn how to use the Cisco Umbrella Investigate API
- Explain the functionality provided by Cisco AMP and its APIs
- Describe how to use Cisco Threat Grid APIs to analyze, search, and dispose of threats

Prerequisites

Before enrolling in this course, you should have professional level knowledge in the following areas:

- Basic programming language concepts
- Basic understanding of virtualization
- Ability to use Linux and Command Line Interface (CLI) tools, such as Secure Shell (SSH) and bash
- CCNP level core networking knowledge
- CCNP level security networking knowledge

The following Cisco courses can help you gain the knowledge you need to prepare for this course:

- **Introducing Automation for Cisco Solutions (CSAU)**
- **Implementing and Administering Cisco Solutions (CCNA®)**
- **Programming Use Cases for Cisco Digital Network Architecture (DNAPUC)**
- **Introducing Cisco Network Programmability (NPICNP)**
- **Implementing and Operating Cisco Security Technologies (SCOR)**

Outline

- Introducing Cisco Security APIs
- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs
- Describing Cisco Security Management Appliance APIs



Lab outline

- Query Cisco AMP Endpoint APIs for Verifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuration
- Automate Firewall Policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct a Report Using Cisco Stealthwatch Cloud APIs

