
6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: <http://www.ctclc.com>

Implementing Automation for Cisco Security Solutions (SAUI) V1.1

The **Implementing Automation for Cisco Security Solutions (SAUI)** 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. This course also earns you 24 Continuing Education (CE) credits towards recertification.

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
- Earn 24 CE credits toward recertification
- Prepares you for the 300-735 SAUTO exam

Objective

Upon completing this course, the student will 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

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 Attend

The primary audience for this course is as follows:

- Network Engineer
- Network Administrator
- Network Manager
- Systems Engineer
- Wireless Engineer
- Wireless Design Engineer
- Consulting Systems Engineer
- Sales Engineer
- Technical Solutions Architect
- Account Manager

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)

Price :
\$2895.00
Duration :
3 Days
Certification Exam:
300-735 SAUTO
CE Credit: 24

Course Outline

Module 1: Introducing Cisco Security APIs

Module 2: Consuming Cisco Advanced Malware Protection APIs

Module 3: Using Cisco ISE

Module 4: Using Cisco pxGrid APIs

Module 5: Using Cisco Threat Grid APIs

Module 6: Investigating Cisco Umbrella Security Data Programmatically

Module 7: Exploring Cisco Umbrella Reporting and Enforcement APIs

Module 8: Automating Security with Cisco Firepower APIs

Module 9: Operationalizing Cisco Stealthwatch and the API Capabilities

Module 10: Using Cisco Stealthwatch Cloud APIs

Module 11: 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