

## Cisco® Protecting Against Malware Threats with Cisco AMP for Endpoints v5.0 (SSFAMP)

### Overview

---

The Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) v5.0 course shows you how to deploy and use Cisco® AMP for Endpoints, a next-generation endpoint security solution that prevents, detects, and responds to advanced threats. Through expert instruction and hands-on lab exercises, you will learn how to implement and use this powerful solution through a number of step-by-step attack scenarios. You'll learn how to build and manage a Cisco AMP for Endpoints deployment, create policies for endpoint groups, and deploy connectors. You will also analyze malware detections using the tools available in the AMP for Endpoints console.

### Prerequisite Comments

---

To fully benefit from this course, you should have the following knowledge and skills:  
Technical understanding of TCP/IP networking and network architecture  
Technical understanding of security concepts and protocols

### Target Audience

---

Security administrators  
Security consultants  
Network administrators  
Systems engineers  
Technical support personnel  
Cisco integrators, resellers, and partners

### Course Objectives

---

After taking this course, you should be able to:

- Identify the key components and methodologies of Cisco Advanced Malware Protection (AMP)
- Recognize the key features and concepts of the AMP for Endpoints product
- Navigate the AMP for Endpoints console interface and perform first-use setup tasks
- Identify and use the primary analysis features of AMP for Endpoints
- Use the AMP for Endpoints tools to analyze a compromised host
- Describe malware terminology and recognize malware categories
- Analyze files and events by using the AMP for Endpoints console and be able to produce threat reports
- Use the AMP for Endpoints tools to analyze a malware attack and a ZeroAccess infection
- Configure and customize AMP for Endpoints to perform malware detection
- Create and configure a policy for AMP-protected endpoints
- Plan, deploy, and troubleshoot an AMP for Endpoints installation
- Describe the AMP Representational State Transfer (REST) API and the fundamentals of its use
- Describe all the features of the Accounts menu for both public and private cloud installations

### Course Outline

---

## 1 - Course Outline

Introduction To Cisco Amp Technologies  
Amp For Endpoints Overview And Architecture  
Console Interface And Navigation  
Using Amp For Endpoints  
Detecting An Attacker — A Scenario  
Modern Malware  
Analysis  
Analysis Case Studies  
Outbreak Control  
Endpoint Policies  
Amp Rest Api  
Accounts

---