



Introducing the Endpoint Update App for the Cisco Application Centric Infrastructure (ACI)

The Endpoint Update App for the Cisco Application Centric Infrastructure (ACI) provides single-click access to all Cisco ACI fabric information, enabling network automation, programmability, and centralized management.

The following topics provide an overview of the ACI endpoint update app and related components.

- [Introduction, on page 1](#)
- [Related Documentation, on page 2](#)

Introduction

The Cisco Application Centric Infrastructure (ACI) is a software-defined network solution and application-intelligent fabric that brings application, security, and infrastructure together in the data center. ACI consists of the following:

- The Cisco Application Policy Infrastructure Controller (APIC) provides single-click access to all Cisco ACI fabric information, enabling network automation, programmability, and centralized management.

To use the system, perform the following tasks in the order shown:

1. Install and configure APIC as discussed in the [Cisco APIC Getting Started Guide](#).
 2. Install and configure the ACI endpoint update app discussed in this guide.
- The ACI endpoint update app periodically retrieves endpoint information from the APIC and pushes it to the Secure Firewall Management Center (formerly Firepower Management Center) and ASA using a REST API. This helps when configuring a security policy on the management center and ASA.

This guide discusses the ACI endpoint update app.

APIC 5.1 introduces a remediation module that quarantines an infected management center so no more traffic is allowed to go in or out of that management center. You do not have to configure anything in the ACI endpoint update app to use this module. For more information, see the [release notes](#).

Related Documentation

- [Cisco Application Centric Infrastructure Fundamentals, ACI App Center](#)
- [Cisco Secure Firewall Management Center Configuration Guides](#)