# Troubleshoot Security Cloud Integration Connectivity Issues on FMC

## Contents

## Issue

Cisco Firewall Management Center (FMC) cannot establish connectivity to Cisco Security Cloud for integration.

## Environment

- Cisco Secure FMC for VMware (applicable to all models)
- Software Version: 7.6.2.1 (applicable to all versions)
- Network environment with upstream security controls/firewall policies

## Resolution

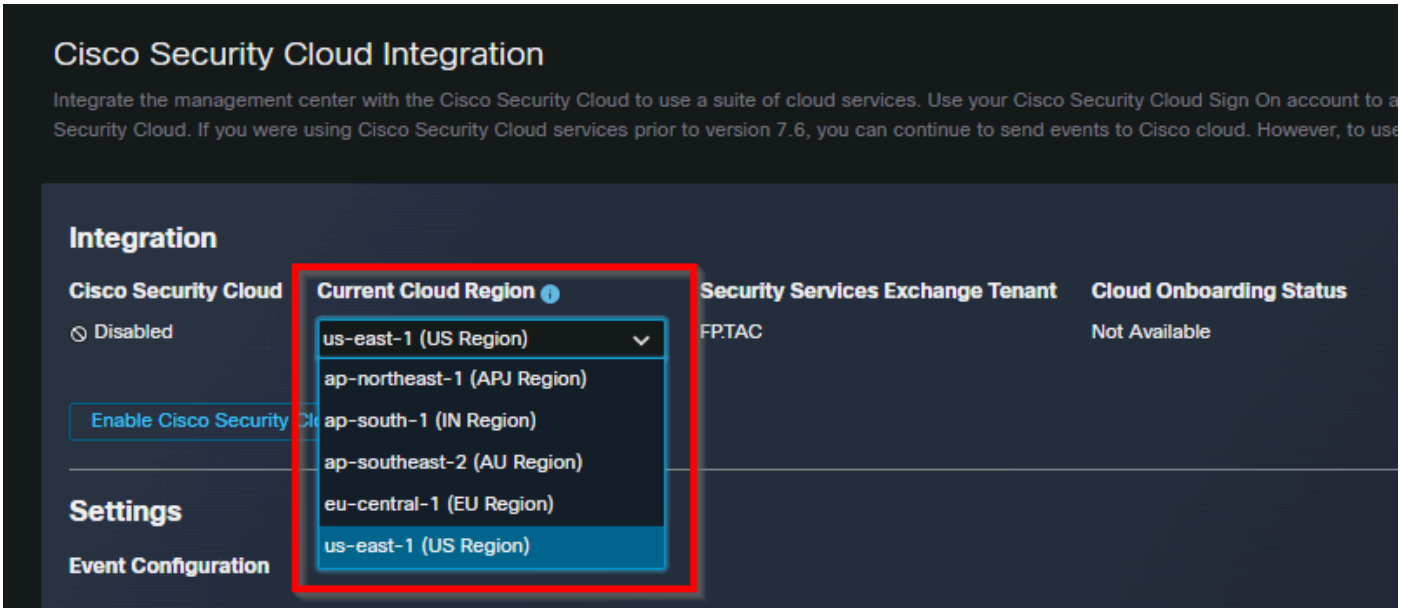
To resolve the Cisco Security Cloud integration connectivity issue, follow these troubleshooting and resolution steps:

1: Test connectivity to the required Cisco Security Cloud URLs using these commands from the FMC as root user:

```
curl -v -k https://www.defenseorchestrator.com
nslookup www.defenseorchestrator.com
telnet www.defenseorchestrator.com 443
curl -v -k https://admin.sse.itd.cisco.com
nslookup admin.sse.itd.cisco.com
telnet admin.sse.itd.cisco.com 443
curl -v -k https://securex.us.security.cisco.com
nslookup securex.us.security.cisco.com
telnet securex.us.security.cisco.com 443
curl -v -k https://api-services.us.sse.itd.cisco.com
```

```
nslookup api-services.us.sse.itd.cisco.com
telnet api-services.us.sse.itd.cisco.com 443
curl -v -k https://api-sse.cisco.com
nslookup api-sse.cisco.com
telnet api-sse.cisco.com 443
curl -v -k https://registration.us.sse.itd.cisco.com
nslookup registration.us.sse.itd.cisco.com
telnet registration.us.sse.itd.cisco.com 443
```

2: If the connectivity tests show connection refusals or forbidden responses, update the upstream network security policies to allow FMC outbound HTTPS access to all required Cisco Security Cloud URLs for the us-east-1 region, if that is the region being used. Ensure these URLs are permitted over TCP port 443 from the FMC to the internet through any intermediate firewalls, proxies, or security controls.




*inline_image_0.png*

- defenseorchestrator.com
- admin.sse.itd.cisco.com
- securex.us.security.cisco.com
- api-services.us.sse.itd.cisco.com
- api-sse.cisco.com
- registration.us.sse.itd.cisco.com

3: After updating the network security policies, retry the Cisco Security Cloud integration from the FMC interface and the curl/telnet commands. The integration now completes successfully with proper access to all required cloud endpoints.

## Cause

The FMC could not reach the Cisco Security Cloud backend services because the required Cisco cloud URLs for the selected region (us-east-1) were not allowed through the network security controls, resulting in HTTPS connection failures during the integration process.

## Related Content

- Manage On-Premises Firewall Management Center with Security Cloud Control
- Cisco Technical Support & Downloads