

Troubleshoot SEG "Either API Server Is Not Started or Is Unreachable"

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

[Related Information](#)

Introduction

This document describes how to troubleshoot the error “Either API server is not started or is unreachable” in Secure Email Gateway (SEG) Next-Gen GUI.

Prerequisites

Starting with AsyncOS 11.4 and continuing with AsyncOS 12.x for Security Management Appliance (SMA), the web user interface (UI) has undergone a redesign as well as the internal processing of data.

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Email Gateway (SEG)
- Security Management Appliance (SMA)
- Web user interface (UI) access

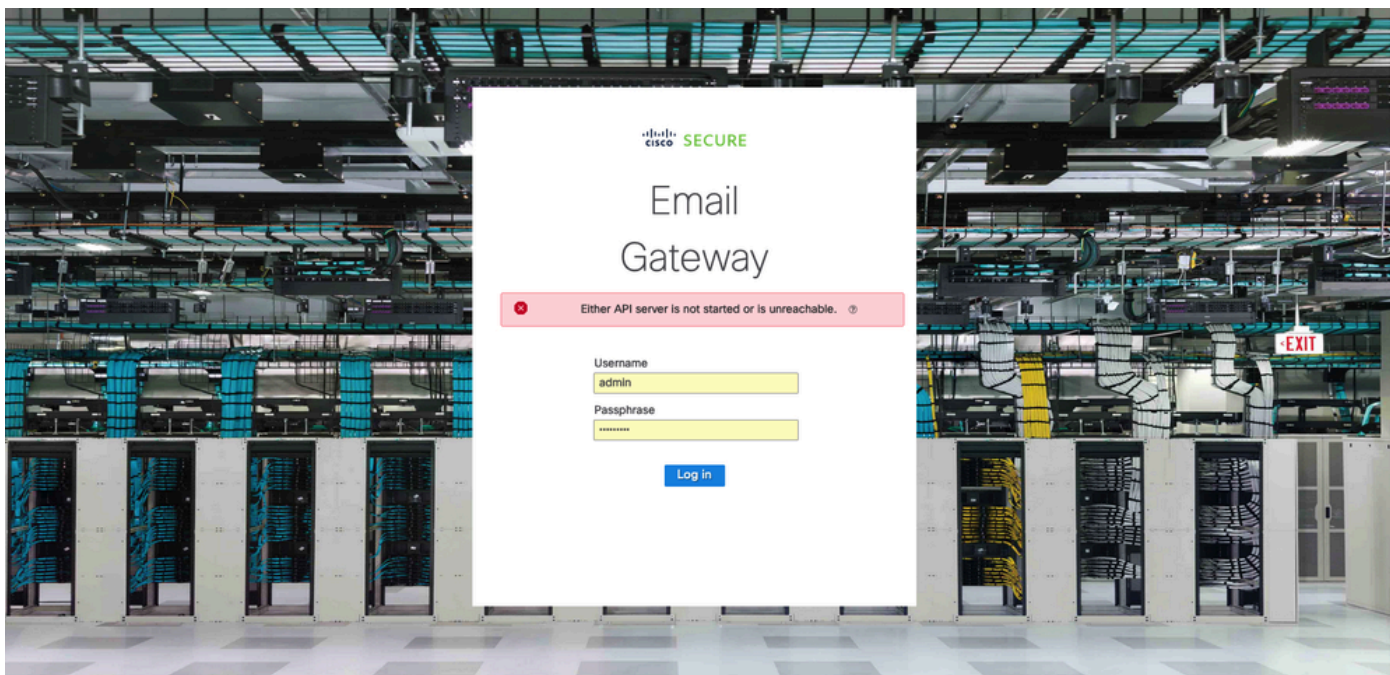
Components Used

- SEG on version 11.4 or later releases
- SMA on version 12.x. or later releases

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.


Problem

Unable to access the Next Generation web interface and getting the error 'Either the API Server is not started or is unreachable'.



Solution

Step 1. Verify that AsyncOS API HTTPS is enabled in the Management IP of the Secure Email Gateway/Security Management Appliance

 **Note:** For Cisco Secure Email Cloud Gateway, contact TAC to review the IP configuration.

```
<#root>
```

```
sma.local> interfaceconfig
Currently configured interfaces:
1. Management (10.31.124.134/26 on Management: esa14.mexesa.com)
```

```
Choose the operation you want to perform:
```

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[> edit
```

```
Enter the number of the interface you wish to edit.
```

```
[> 1
```

```
IP interface name (Ex: "InternalNet"):
```

```
[Management]>
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
```

```
IPv4 Address (Ex: 192.168.1.2 ):
```

```
[10.31.124.134]>
```

```
Netmask (Ex: "24", "255.255.255.0" or "0xffffffff"): 
```

```
[0xffffffffc0]>
```

```
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
```

Ethernet interface:

1. Management

[1]>

Hostname:

[sma.local]>

Do you want to configure custom SMTP Hello to use in the SMTP conversation? [N]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

[22]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable Cluster Communication Service on this interface? [N]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?

[80]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?

[443]>

Do you want to enable Spam Quarantine HTTP on this interface? [N]>

Do you want to enable Spam Quarantine HTTPS on this interface? [N]>

Do you want to enable AsyncOS API HTTP on this interface? [N]>

Do you want to enable AsyncOS API HTTPS on this interface? [N]> Y

Step 2. Confirm the hostname configuration

Ensure the appliance hostname is not in use in any other configuration or appliance, run the **sethostname** command to verify it or change the configuration if needed.

```
<#root>
```

```
sma.local>
```

```
sethostname
```

```
[sma.local]>
```

Step 3. Verify network access

For Next Generation GUI, is required to allow trailblazer and port 443.

Run the command **trailblazerconfig status**.

```
<#root>
```

```
sma.local>
```

```
trailblazerconfig status
```

```
trailblazer is not running
```

```
sma.local>
```

```
trailblazerconfig enable
```

```
trailblazer is enabled.
```

Step 4. Access the Next Generation GUI

Access the Next Generation web interface.

If the issue persists contact Cisco TAC.

Related Information

- [Disable/Enable New-GUI Banner on Security Management Appliances](#)
- [Administrative details on 'trailblazer' CLI command for Cisco Security Management Appliance \(SMA\)](#)