

ISE Email Alarm Notifications Not Working After Software Upgrade

Contents

Issue

Cisco Identity Services Engine (ISE) email alarm notifications are not being delivered to configured recipients. The SMTP test function within ISE succeeds, but actual alarm events do not trigger email notifications to be sent. This issue began occurring after upgrading from ISE version 3.2 to 3.4 Patch 3, and persisted even after applying 3.4 Patch 5. The alarm emails worked briefly immediately after applying Patch 5 but stopped functioning again when the email notifications were re-enabled after being temporarily disabled due to high volume.

Environment

- Cisco Identity Services Engine (ISE) version 3.4 Patch 5
- ISE deployment with 6 Policy Service Nodes (PSNs), 2 Monitoring & Troubleshooting (MnT) nodes, and 2 Policy Administration Nodes (PANs)
- Primary MnT node: COR089ISE-MnT02 (IP: 172.29.134.2)
- SMTP server: smtp1.us.parker.corp
- Previous working configuration on ISE version 3.2
- Issue started after upgrade from version 3.2 to 3.4 Patch 3 in October

Resolution

To troubleshoot ISE email alarm notification issues, follow the diagnostic and resolution steps described in the next sections.

Step 1: Verify SMTP Configuration and Test Functionality

Confirm that the SMTP test within ISE is successful and verify the email server configuration:

1. Navigate to **Administration > System > Settings > SMTP Server** in the ISE GUI.
2. Verify all SMTP settings including server address, port, TLS/STARTTLS configuration, and authentication settings.
 - Ensure the IP address or FQDN of the SMTP Server (Mail Gateway) is correct.
 - Check the **SMTP Port**: Default is port 25. If secure transmission (TLS/STARTTLS) is enabled, it must explicitly match the open port on the email server (such as port 587).
3. Test the SMTP connection using the built-in test function.
4. Coordinate with the email server administrators to confirm whether test emails are being received at the server level.

Step 2: Enable Debug Logging on Primary MnT Node

Use root access to isolate whether the issue is an internal trigger success or an external connection error with the server:

```
tail -F /opt/CSC0cpm/logs/ise-psc.log
2026-06-02 14:51:54,851 WARN [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,851 INFO [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,853 ERROR [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
```

If further troubleshooting is required or you are unable to monitor via root, enable detailed logging to capture alarm generation and email delivery attempts.

Enable these debug components on the Primary MnT node:

```
cisco-mnt
cpm-mnt
```

Step 3: Capture Network Traffic During Alarm Events

Perform packet capture to verify whether ISE attempts to establish SMTP connections for alarm events:

1. Navigate to **Operations > Troubleshoot > Diagnostic Tools > TCP Dump** on the Primary MnT node.
2. Select the network interface used to communicate with the SMTP server.
3. Start the packet capture.
4. While capturing, perform both:
 - Run the SMTP test from ISE (to capture known-good SMTP session).
 - Generate or wait for an actual alarm event to occur.
5. Stop the capture and download the PCAP file for analysis.

Step 4: Monitor Application Logs During Alarm Generation

Monitor ISE application logs to identify email sending attempts.

Run this command on the Primary MnT node CLI while an alarm is being generated:

```
show logging application ise-psc.log tail
```

Capture the output and note the timestamp of any alarm events that need to trigger email notifications.

Step 5: Coordinate with Email Server Administration

Work with email server administrators to verify server-side processing.

During alarm testing, have the email team check the SMTP server logs for:

- SMTP connections from the Primary MnT node IP address
- Message acceptance, rejection, or deferral status

- Any error codes or rejection reasons if messages are not accepted

Step 6: Analyze Captured Data and Implement Resolution

Review the collected packet captures, logs, and server-side information to determine:

- Whether ISE is attempting to send alarm emails (visible in packet capture).
- Server response codes and any rejection reasons.
- Differences between successful SMTP test sessions and alarm-triggered sessions.

Based on the analysis, implement appropriate fixes such as:

- Adjusting SMTP server configuration or security policies.
- Modifying ISE email notification settings.
- Updating sender address or authentication parameters.

Step 7: Disable Debug Logging

After completing troubleshooting, disable the debug logging components to prevent log file growth.

Disable the debug components on the Primary MnT node:

```
cisco-mnt (disable)
cpm-mnt (disable)
```

Cause

The issue can stem from differences in how the Primary Monitoring & Troubleshooting (MnT) node handles SMTP sessions for alarm events versus SMTP test functions. While the SMTP test succeeds, the actual alarm-triggered email attempts can fail due to configuration incompatibilities, server-side filtering, or changes in the email sending process introduced in the newer ISE version.

Related Content

- [Cisco ISE 3.4 Administration Guide - Troubleshooting](#)
- [Cisco Technical Support & Downloads](#)