Revised: June 6, 2025

Cisco Nexus Hyperfabric — Notifications

Notifications

Set up notifications to receive alerts about fabric-related events and their significance. Notifications can help monitor and maintain the health of the fabric.

Currently, the default policy notification enables the configuration of assertion notifications for one or more fabrics and the notification endpoints you specify. See Configure notifications, on page 6.

Notification endpoints

Notification endpoints allow the system to send alerts or updates to a designated recipient or endpoint. A notification endpoint can be an application, service, or a user that receives these notifications.

Cisco Nexus Hyperfabric currently supports these notification endpoint types:

- email
- Amazon S3

Assertion notification content and frequency

The content and delivery of assertion notification information vary depending on the notification endpoint type.

Notifications are sent only when there are changes in latched assertions. Notifications follow two timing methods: a short window of 30 seconds and a long window of five minutes. For instance, if no state changes occur after a notification, the next one is sent in five minutes. However, if a state change happens within five minutes, the next notification is sent 30 seconds after the last one.

Configure email endpoints

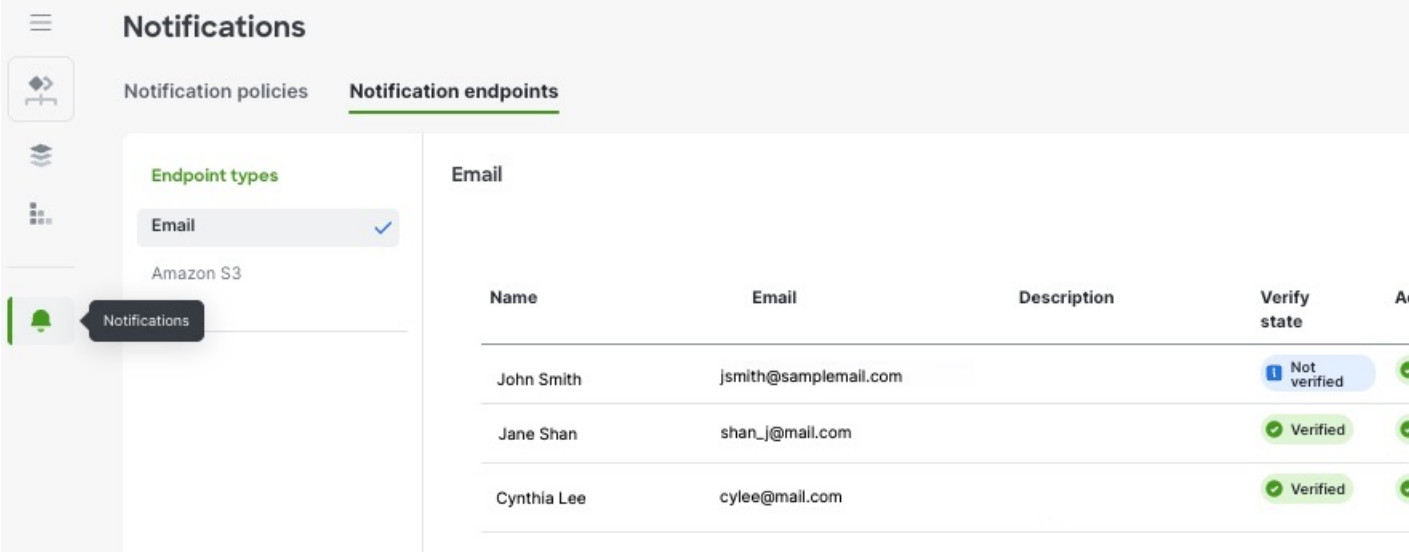
The system sends a verification code to the email address you configure. Ensure you have access to the email address or can retrieve the verification code by another means. Notification codes remain valid for 30 minutes. After this time, the email code will expire and you need to request a new one.

Follow these steps to configure email endpoints.

Step 1 Choose **Notifications** > **Notification endpoints**.

Step 2 From the **Endpoint types** area, click **Email**.

Step 3 Click **+ Add**.



Step 4 In the **Add email endpoint** window, enable or disable notifications for this email endpoint. Notifications are enabled by default.

Step 5 Enter a name, email address, and a description.

Step 6 Click **Save**.

Step 7 Complete email verification.

a) Retrieve the verification code that was sent to the email address you just configured.

b) Enter the verification code and click **Verify**.

c) From the **Endpoint Email Summary** page, confirm that the email is verified and active.

Step 8 If you want to configure more email endpoints, repeat these steps.

Step 9 If you want to send notifications using this email endpoint, see Configure notifications, on page 6.

Example

Figure 1: Similar email content

From: Cisco Hyperfabric
Date: Friday, May 9, 2025 at 5:36 PM
To: John Smith
Subject: Cisco Hyperfabric Assertions Summary

You are subscribed to notifications from Cisco Hyperfabric.

The following assertions have been raised. Note that only a subset of assertions will be displayed for each impacted fabric. For the full list please click on the embedded link for the fabric.

There are 4 assertions for fabric: **Fabric-ABC**

Type:	Port link is unexpectedly down
Status:	Critical
Modified at:	May 29, 2025 08:06:53PM
Port name:	Ethernet1_1
Device id:	48-80-02-99-c6-d0
Target device id:	98-d7-e1-00-60-00
Target port name:	Ethernet1_31

Type:	Switch is not connected to cloud
Status:	Critical
Modified at:	May 29, 2025 08:07:04PM

Type:	Port link is unexpectedly down
Status:	Critical
Modified at:	May 29, 2025 08:07:04PM
Port name:	Ethernet1_32
Device id:	98-d7-e1-00-c8-00
Target device id:	48-80-02-99-c7-58
Target port name:	Ethernet1_2

Type:	Switch is not connected to cloud
Status:	Critical
Modified at:	May 29, 2025 08:07:13PM

Please visit Cisco Hyperfabric for more information.

Thank you for your business,

Cisco Hyperfabric

Note

The email contains a subset of prioritized assertions per fabric. Click on the fabric name to display all fabric-related assertions in the UI.

Configure Amazon S3 endpoints

You can send notifications to an existing Amazon Simple Storage Service (Amazon S3).

Ensure you have the required Amazon S3 information:

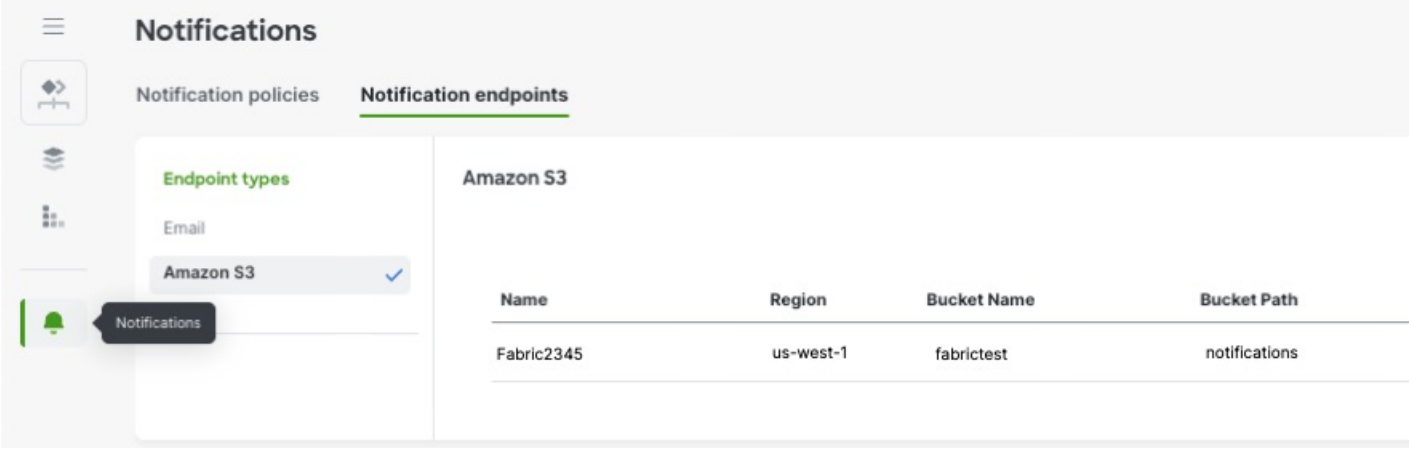
- AWS region
- bucket name
- bucket path, and
- Amazon Web Services (AWS) access key ID and corresponding secret access key

Follow these steps to configure notifications for Amazon S3 endpoints.

Step 1 Choose **Notifications** > **Notification endpoints**.

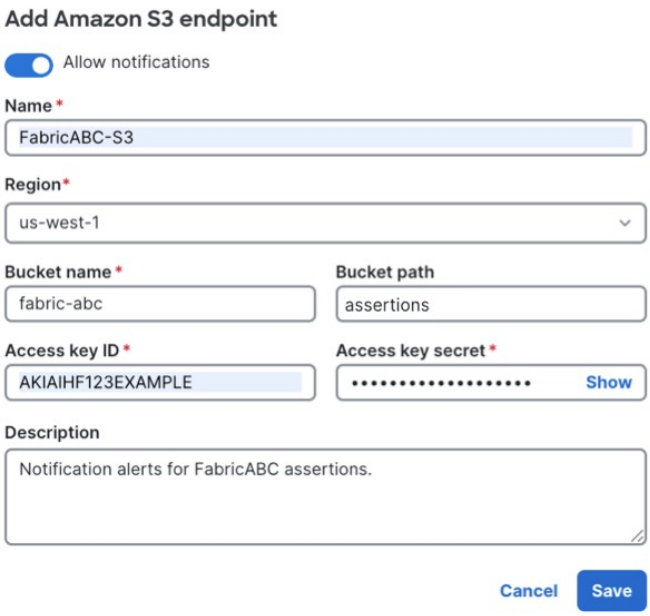
Step 2 From the **Endpoint types** area, click **Amazon S3**.

Step 3 Click **+ Add**.



Step 4 In the **Add Amazon S3 endpoint** window, enable or disable notifications for this endpoint. Notifications are enabled by default.

Step 5 Enter a name for the endpoint and the required AWS information.



Step 6 Click **Save**.

Step 7 If you want to configure more Amazon S3 endpoints, repeat these steps.

Step 8 If you want to send notifications using this Amazon S3 endpoint, see Configure notifications, on page 6.

Example

Figure 2: Similar Amazon S3 content


```
{
 "assertions": [
  {
   "assertType": "PORT_EXPECTED_NEIGHBOR",
   "state": "LATCHED",
   "portExpectedNeighbor": {
    "category": "ASSERT_CATEGORY_FABRIC",
    "assertState": "ASSERT_STATE_FALSE",
    "modifiedAt": "2025-05-12T23:28:55.545033173Z",
    "config": {
     "latchedAt": "2025-05-12T23:21:31.778298918Z",
     "port": {
      "portName": "Ethernet1_1",
      "portIndex": 1,
      "portRole": "FABRIC_PORT",
      "adminState": "DISABLED",
      "mtu": 9216,
      "deviceId": "02-17-dd-76-01-00",
      "targetDeviceId": "02-17-4d-c0-00-00",
      "targetPortName": "Ethernet1_1",
      "modifiedAt": "2025-05-12T23:28:49.074929086Z"
     },
     "fabricId": "a40c5574-03ab-4bf9-8f31-8f4133a58339"
    },
    "readyToLatchAt": "2025-05-12T23:21:31.778298918Z"
   }
  }
 ]
}
```


The notification is sent as a JSON file with the filename format as **notification_<*endpoint-name*>-<*timestamp*>.json**.

Configure notifications

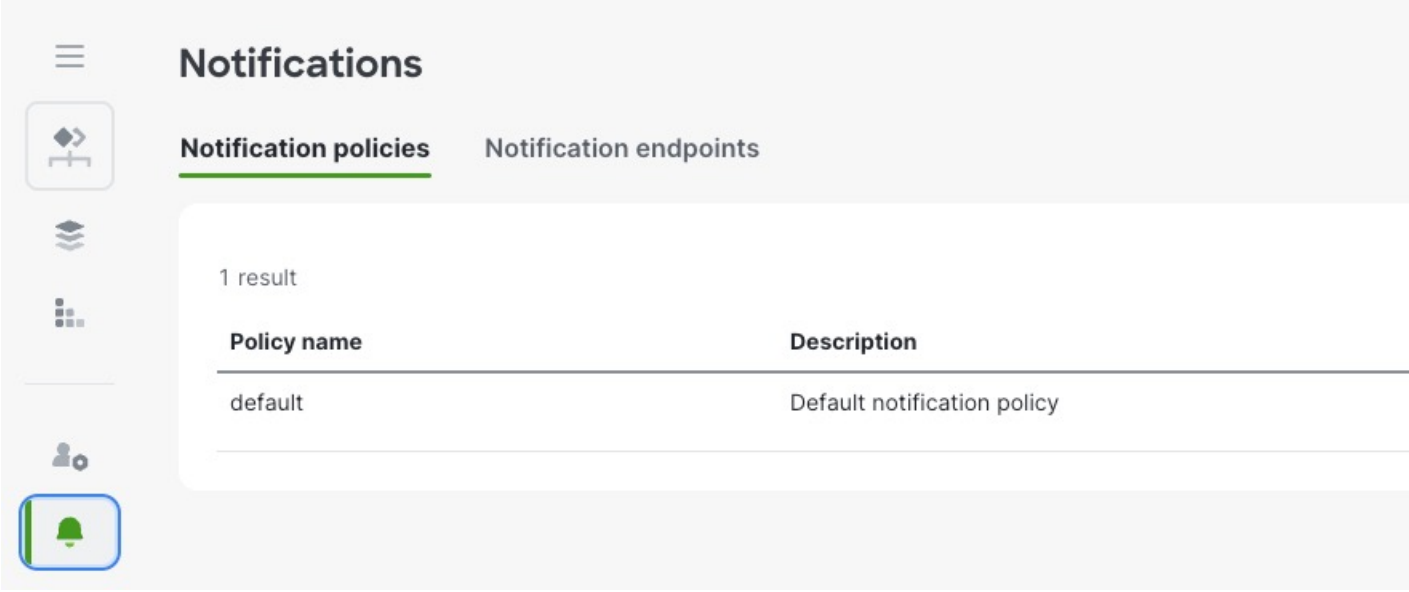
At this time, you can set up notifications only for specific fabrics to designated endpoints using the default policy. Additionally, different notification policies can be created for various fabrics and notification endpoints.

Ensure you have configured a notification endpoint before you configure notifications.

Follow these steps to configure notifications.

Step 1 Choose **Notifications** > **Notification policies**.

Step 2 Under the **Action** column, click the pencil icon.



Step 3 Click +.

Step 4 From the **Fabrics** drop-down list, select one or more fabrics for which you want to receive assertion notifications for.

Step 5 From the **Endpoints** drop-down list, select one or more endpoints for which you want to send assertion notifications to.

Step 6 Click **Save**.

Step 7 If you want to configure more assertion notification policies with different fabric and endpoint combinations, click +.