ServiceNow Instance Observer – Lightstep Incident Response integration

QuickStart Guide

Table of Contents

Lightstep
from ServiceNow

Introduction

This document provides a step-by-step plan to:

- Integrate ServiceNow Instance Observer with Lightstep Incident Response
- Configure Lightstep Incident Response
- Send a ServiceNow Instance Observer sample alert to test Incident Response

Prerequisites

- ✓ ServiceNow Instance Observer version 10.0
- ✓ A subdomain name to create your Lightstep Incident Response tenant instance
- ✓ ServiceNow single sign on (SSO)

Integration setup

As an Instance Observer user, you must first set up the integration with Lightstep Incident Response using the following steps:

1. Create the ServiceNow Instance Observer – Lightstep Incident Response integration
2. Add or invite users in Lightstep Incident Response
3. Ask invited users to set up their Lightstep Incident Response profile
4. Assign users to a team in Lightstep Incident Response
5. Configure the team on-call scheduling in Lightstep Incident Response
6. Configure the team escalation policy in Lightstep Incident Response
7. Configure the services assigned to the team
8. Disable email notification from ServiceNow Instance Observer
9. Send a sample alert from ServiceNow Instance Observer

First Instance Observer user to log in to Incident Response

1. Create the ServiceNow Instance Observer – Lightstep Incident Response integration

Automate various actions from Instance Observer into Lightstep Incident Response, like automatically creating a Lightstep Incident Response tenant instance, creating a webhook, and configuring it in Instance Observer.

1. Initiate the integration from ServiceNow Instance Observer:
    a. Navigate to **Instance Observer** > **Alerts** > **Configure Notification** and click **Configure Lightstep Incident Response**.
    b. Enter the **subdomain** and click on **Check availability**. Pick another subdomain name if the one you selected is not available.
    c. Accept the **Terms of Service** and click **Configure**.
    d. Your tenant instance is created automatically with the following defaults:
        - An Administrator user account for the user setting up the integration. This account is assigned the email address for that user and as the only notification preference.
        - A team with that user as the only team member, with an on-call schedule having that user on call 24x7, and a simple escalation policy to be notified for all alerts and incidents for any of the five priorities P1 through P5 (P1 = critical, P2 = major, P3 = minor, P4 = warning, P5 = informational).
        - Every ServiceNow instance monitored by Instance Observer is instantiated as a service in Lightstep Incident Response. This allow alerts from different ServiceNow instances to be assigned to different teams.

2. Send a test alert from Instance Observer.
   The configured user should receive an email for that test alert.

You have completed the integration of Lightstep Incident Response with Instance Observer. Now, you must:

- Add users to your team and have them set their notification preferences.
- Specify the team on-call schedule and escalation policies.
- Assign services to the team.

2. Add or invite users in Lightstep Incident Response

Whether you have only one team or multiple teams being responsible to process Instance Observer alerts, you need to add more responders.

1. Select **Users** from the navigation pane.
2. Select **Invite users** and enter one or more comma-separated email addresses, then press **Enter**.
3. Assign each user the correct role of Manager, Responder, or Stakeholder.
4. Click **Send invite**. The users are added to Incident Response with the status of *Invited, not signed up yet*.
5. Each user you invited will receive an email invitation to log in to Incident Response and set up their profile. Alternatively, they may log in Instance Observer and:
    a. Select **Alerts** > **Configure Notification**.
    b. Click **Configure Lightstep Incident Response**.
       You will see the subdomain.
    c. Accept the **Terms and Conditions** to be automatically logged in to LIR using SSO.

3. Ask invited users to set up their Lightstep Incident Response profile

Ask every invited user to set up their profile and notification preferences.

1. Once logged in to Lightstep Incident Response, select **Users** and your user tile.
2. Click **Edit profile** and specify:
    - Title (optional)
    - Email (will be already defined and not editable)
      Click **Add new** to add another email address.
    - Phone: Enter a phone number to be notified by a phone call
      Click **Add new** to add another phone number
    - SMS: Enter a phone number to receive SMS messages (carrier charges may apply)
      Click **Add new** to add another phone number to receive SMS messages.
    - Tags (optional)
    - What I do here (optional)
3. Click **Save**.
4. Click **Change avatar** to select an avatar or upload an image.
5. Click **Notifications**.
   For each alert or incident priority, specify your preferred notification preferences.

For example, for P1 and P2 alert/incident priorities, you may want both email, SMS, and a phone call, assuming you specified an SMS number and a phone number. For P2 alert/incident priorities, you may only want email.

4. Assign users to a team in Lightstep Incident Response

Assign all users to the team that was automatically created during the initial integration setup. To create multiple teams, see the Advanced topics.

1. Select **On-call teams** from the navigation pane.
2. Select the team tile.
3. Select **Members**.
4. Click **Add members.**
5. Start typing the names of all the users you invited. As you start typing their names, the pull down shows the selections.

5. Configure the team on-call scheduling in Lightstep Incident Response

Define who is on call at any time during weekends and weekdays, and who is the backup. This determines who is notified first when an alert is received.

1. Select **On-call teams** from the navigation pane.
2. Select the team tile. The team on-call schedule appears and shows one user on call 24x7, 7 days a week. Let's change this.
3. Click **Edit** for the Weekday schedule. A panel on the right opens up.
4. Select to **Rotate every 1 Day.**
5. Replace the primary responder by another team member and add a backup responder. For example, Joe is the primary on-call person during the week with Alicia as backup, while Alicia is primary on weekends with Joe as backup.

> **Note:** *The primary team member should have their notification preferences set with at least SMS phone number so that the first alert will be sent as an SMS message to that user.*

6. (Optional) Create another group.
   Add another team member as a responder to create another shift and add a backup responder. You may repeat this step as needed to share the on-call schedule across several groups.
7. Click **Save**.
8. Click **New shift**.
9. Name it Weekends.
10. Select Saturday and Sunday and de-select Monday thru Friday.
11. Select **Rotate every 1 Day**.

12. Create a group.
    Add another team member as a responder and add a Backup responder.
    You may repeat this step as needed to share the on-call schedule across several groups.

You will see **Total coverage** cover every day of the week.

6. Configure the team escalation policy in Lightstep Incident Response

Define how the primary on-call team member are notified and the policy in case the on-call person does not respond, and so on. For example, notify the primary first, then the backup if the primary does not acknowledge the alert within 5 minutes.

1. Select **On-call teams** from the navigation pane.
2. Select the team tile.
3. Select **Escalation policies**.
4. Deselect **Enable reminders**.
5. Click **Edit.**
6. Click **Add an escalation policy**.
7. Choose a time interval, specify the persons to notify in a team.
8. Repeat steps 6 and 7 until satisfied.
9. Click **Save**.
10. Verify that the escalation policy is what you expect.

7. Configure the services assigned to the team

Define the services for which the team is responsible. A service in Lightstep Incident Response corresponds to a ServiceNow instance monitored by ServiceNow Instance Observer.

1. Select **On-call teams** from the navigation pane.
2. Select the team tile.
3. Select **Services**.
4. In the **Unassigned** tab, select all services and click **Assign services.**

You have now completed the configuration of Lightstep Incident Response. So, let's send a sample alert and see what happens, namely that the primary on-call responder is notified according to their notification preferences.

8. Disable email notification from ServiceNow Instance Observer

Disable sending email notifications from Instance Observer alerts and enable notifications from Lightstep Incident Response.

1. In Instance Observer, navigate to **Instance Observer** > **Alerts** > **Configure Notification**.
2. For each Rule in Instance Observer:
    a. Click the **Edit** icon (…).
    b. Disable **Instance Observer Email**.
    c. Enable **Lightstep Incident Response notifications**.

9. Send a sample alert from ServiceNow Instance Observer

Send a sample alert to verify the team on-call scheduling you just created, without having to wait for an Instance Observer to monitor and detect an alert condition.

1. In Instance Observer, navigate to **Instance Observer** > **Availability** > **Self-serve alerts**.
2. Select an instance from the list and click **Get Snapshot**.
   You can see a table with recent alerts appears and a Generate Test Alert button.
3. Click **Generate Test Alert** and select the alert type from the list to generate a sample alert.
4. Go to Lightstep Incident Response and you will see the alert in the Home page and in the Alerts page.

Other users can now log in to Lightstep Incident Response either from ServiceNow Instance Observer or directly to Lightstep Incident Response.

Other Instance Observer users to log in to Incident Response

Once the integration is completed, other users can access Incident Response from Instance Observer as follows:

1. Navigate to **Instance Observer** > **Alerts** > **Configure Notification** and click **Configure Lightstep Incident Response**.
   You can see the Incident Response domain defined during set up.
2. Accept the Terms of Service.
3. Click **Accept & Continue**.
4. Click **Go to Lightstep Incident Response**.
   You are taken to the Log in panel of Incident Response with your email address filled in.
5. Click **Next**.

> ***Note:*** *Because you are already logged in to Instance Observer, you are automatically authenticated into Incident Response using ServiceNow SSO. You should now see the Incident Response home page.*

6. Click **On-call teams**.
7. Click the team tile to open the team details.
8. Select the **Members** tab.
   You must add yourself as a member of the team.
9. Click **Add members** and invite yourself.
10. Click **Add members** to invite other users.
    They will receive an email to log in and set up their profile.

Users logging in directly to Incident Response

You can log in directly if you received an email with an invitation to log in to Lightstep Incident Response. To use ServiceNow SSO, you need a ServiceNow ID.

- If you do not have a ServiceNow ID:
  You would have received 2 emails, one from ServiceNow SSO and one from Incident Response.
  a. First open the email from ServiceNow SSO to accept the invitation and sign up to ServiceNow SSO.
  b. Then open the email from Lightstep Incident Response for informational purposes.
  c. Proceed to the next section once you have a ServiceNow ID.
- If you already have a ServiceNow ID:
  a. Click the link in the email from ServiceNow SSO.

b. Accept the Terms of Service in the new panel. You are then automatically logged in to Incident Response via ServiceNow SSO, and you can see the Incident Response Home page.
c. For information purposes, you will get an email from ServiceNow SSO to inform you that you have been assigned to a new tenant application.

Advanced topics

Setting user notification preferences as Slack or MS Teams channel

This feature allows you to receive a notification on a specific Slack or MS Teams channel.

1. Ask your Lightstep Incident Response administrator to set up Slack or MS Teams.
2. Then, select **Users**.
3. Select your user tile.
4. If Slack is set up, click **Add Slack** and specify the Slack channel you wish to use to be notified of alerts. Once set up, you should see your email address for Slack notifications.
5. If MS Teams is set up, click **Add Microsoft Teams**, and specify the MS Teams channel you wish to use to be notified of alerts. Once set up, you should see your email address for MS Teams notifications.

Splitting services to multiple teams

This feature allows you to assign different services to different teams.

1. Log in to Lightstep Incident Response.
2. Unassign the services that you want to assign to the new team:
    a. Select **On-call teams** from the navigation pane.
    b. Select the team you have used so far.
    c. Click the **Services** tab.
    d. Unassign the services you want to assign to the new team.
3. Create another team. You may invite users or create a new team from the users already configured in Lightstep Incident Response.
4. Assign services to the new team:
    a. Select **On-call teams** from the navigation pane.
    b. Select the team you just created.
    c. Click the **Services** tab.
    d. Click the **Unassigned** tab in Services.
    e. Select and assign the services you want to assign to the new team.

LS-InstanceObserverIntegration-102022

Lightstep.com