FORESCOUT®

Forescout and Slack Integration

08.15.19 - v1.0

—

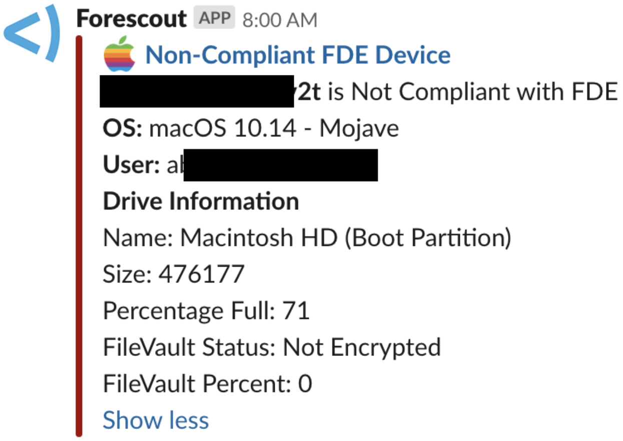
Nick Duda
nduda78@gmail.com
Twitter: @nduda78
LinkedIn: https://www.linkedin.com/in/nickduda/

Summary

Using the Forescout Open Integrations Module (OIM), this document will walk you through integrating Forescout with Slack. Slack is a cloud-based, team collaboration tool suite. With this integration you will gain the following:

1. Post to a Slack Channel
    a. Similar to the *Send Email* action, this action will post whatever you put in the json to the slack channel you pick.
    b. Hyperlink assets in the slack post to the Forescout Asset Portal
2. Post as a direct message to a slack user

With this integration you gain another, real-time, notification method on top of email. The send email action does not allow for HTML, therefore sending hyperlinks is not possible. Using slack you can immediately get alerted to policy triggers with hyperlinked actions in the slack post. Tags {tags} can be used in the json that posts into the slack channel as well.



Forescout APP 8:00 AM

Non-Compliant FDE Device

[redacted]**2t** is Not Compliant with FDE

OS: macOS 10.14 - Mojave

User: a[redacted]

Drive Information

Name: Macintosh HD (Boot Partition)

Size: 476177

Percentage Full: 71

FileVault Status: Not Encrypted

FileVault Percent: 0

Show less

In the example above, the blue text is hyperlinked (asset portal) to the device that triggered the slack post.

Requirements

Forescout Requirements

1. Forescout CounterACT v7.x/8.x
2. Open Integrations Module (OIM - Extended Module)

Slack Requirements

1. A Slack Workspace
    a. You can sign up for a free workspace at www.slack.com
2. Building a custom slack app for Forescout (https://api.slack.com/)

Configuration

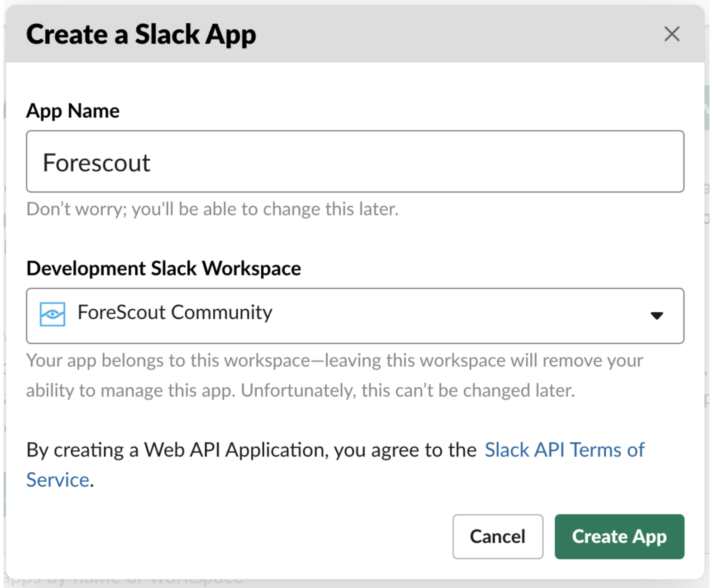
Creating a Slack Workspace

1. Navigate to www.slack.com
2. Sign-up for a slack workspace

Creating the Slack App

1. Navigate and login to https://api.slack.com/
    a. You'll want to login to the slack workspace you want to integrate with.
2. Click on the Start Building icon to build a new app
3. Create a Slack App
    a. Give your app a name (i.e. Forescout)

b. Select the workspace for the app



Create a Slack App

App Name

Forescout

Don't worry; you'll be able to change this later.

Development Slack Workspace

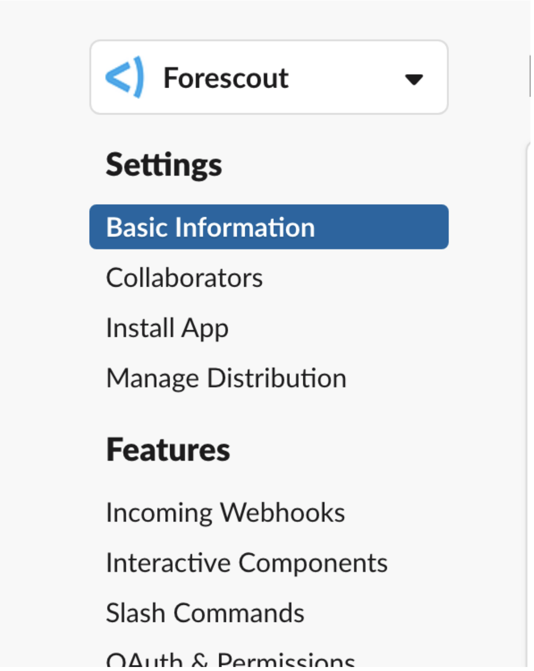
ForeScout Community

Your app belongs to this workspace—leaving this workspace will remove your ability to manage this app. Unfortunately, this can't be changed later.

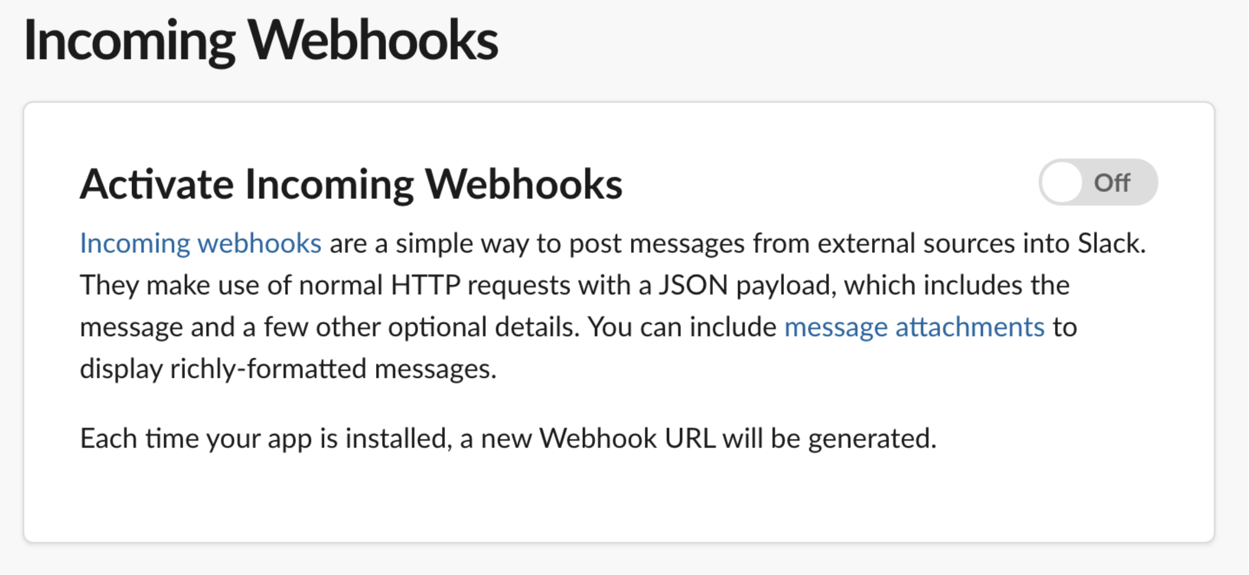
By creating a Web API Application, you agree to the Slack API Terms of Service.

c. Click Create App

4. You'll now be in the configuration section for the App you created. Click on Incoming Webhooks in the list.



5. Enabled the Webhook by flipping the switch to On



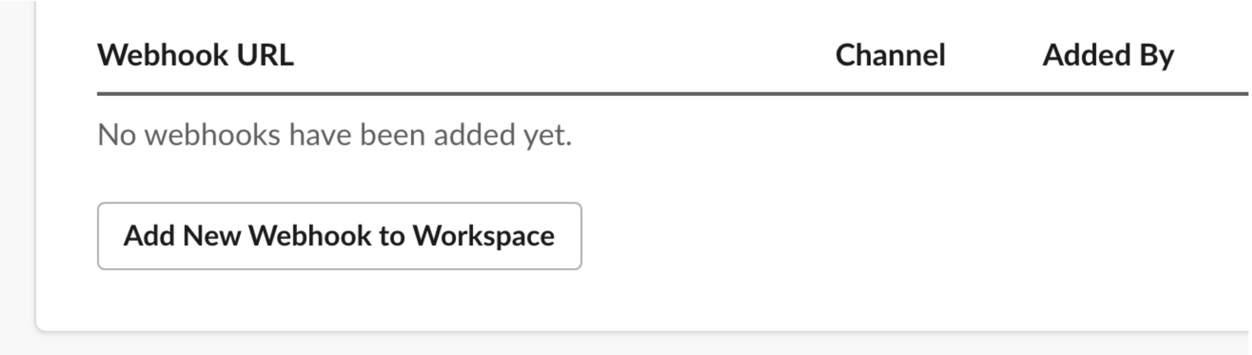
Incoming Webhooks

Activate Incoming Webhooks

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include message attachments to display richly-formatted messages.

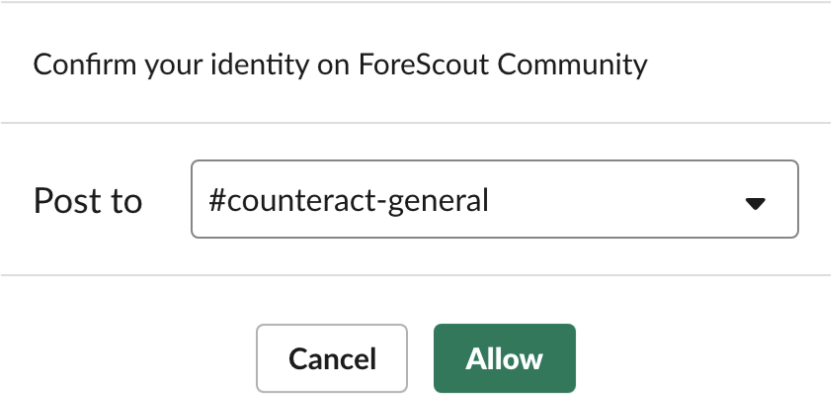
Each time your app is installed, a new Webhook URL will be generated.

6. Click the Add New Webhook To Workspace button at the bottom



Webhook URL	Channel	Added By
No webhooks have been added yet.		

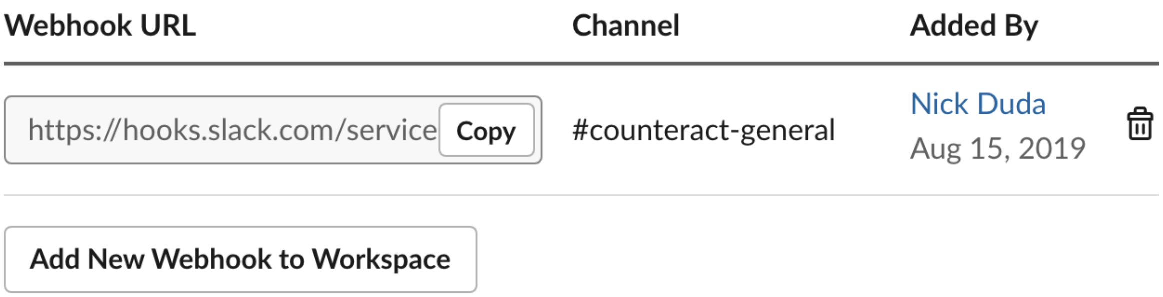
7. Select the Channel or User you want this webhook to post to and click Allow:



Confirm your identity on ForeScout Community

Post to: #counteract-general

8. Once you click Allow you should see a slack message in the channel you selected stating a new integration was made.
9. Back on the webhook page at the bottom is the URL you will use in Forescout to post to this webhook. **Make a note of it! Also don't share it with anyone as they will be able to use it to post into the channel as well.**

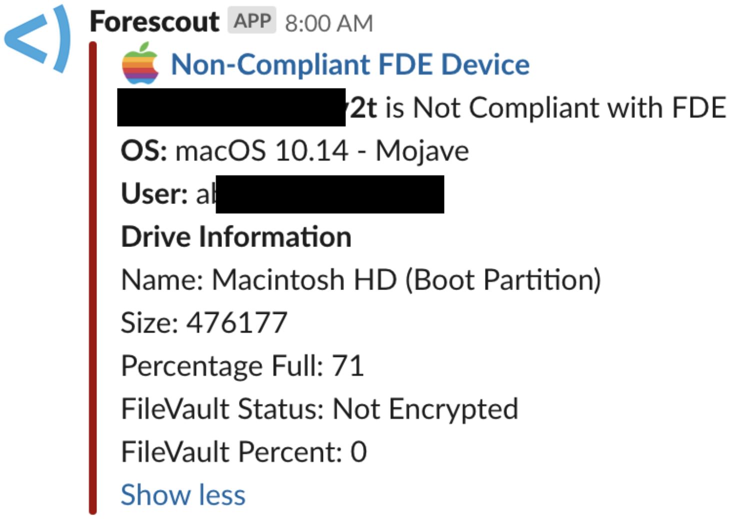


Webhook URL	Channel	Added By
https://hooks.slack.com/service Copy	#counteract-general	Nick Duda Aug 15, 2019

Create the action to post into the Slack Channel (webhook)

1. In the Forescout Console, navigate to the policy/sub-rule you want to perform the slack post action to.
2. Add the *DEX Send Web Service Request* action.
    a. Action Identifier: This can be whatever you want, I like to use the name of the slack channel this will post into.
    b. HTTP Method: POST
    c. Request URL: This is the Webhook URL from Step 9 in the last section.
    d. HTTP message headers (raw): Content-Type: application/json
    e. HTTP message body: This is where you will post the slack json that you want posted in the slack channel when the action is performed. To learn about all the options you can use in the json please see https://api.slack.com/messaging

The example json below is what I use to generate this slack post. I'm using this example to show how I'm using {tags} from yet another integration I have with JAMF:



Forescout APP 8:00 AM

Non-Compliant FDE Device

[redacted]**2t** is Not Compliant with FDE
OS: macOS 10.14 - Mojave
User: al[redacted]
Drive Information
Name: Macintosh HD (Boot Partition)
Size: 476177
Percentage Full: 71
FileVault Status: Not Encrypted
FileVault Percent: 0

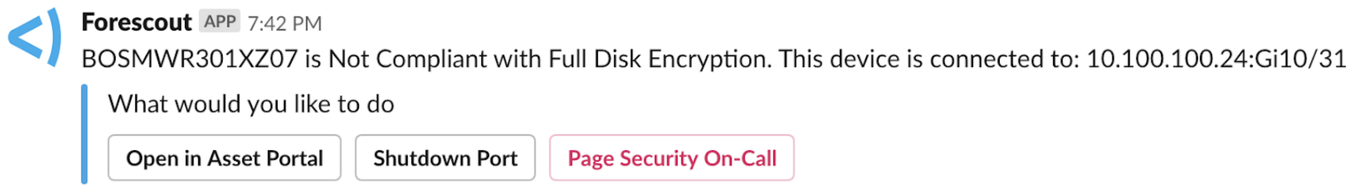
```
{
        "icon_emoji":":counteract:",
        "attachments":[
                {
                "fallback":"Non-Compliant FDE Device!",
                "color":"danger",
                "title":":apple-icon: Non-Compliant FDE Device",

"title_link":"https://APPLIANCE_OR_EM/assets/rangesearch?main_selection=ip&query={ip}&address={ip}",
                "text":"*{dhcp_hostname}* is Not Compliant with FDE\n*OS:* {os_classification}\n*User:*
{dexextweb_jamf_local_users}\n*Drive Information*\n{dexextweb_jamf_boot_device}",
                }
]
}
]
}
```

The icon_emoji can be any emoji in your slack workspace. I created one for :counteract: by uploading the Forescout logo. The title_link is what links to the asset in the Asset Portal.

Another json example for Windows based running Peer-to-Peer software:

```
{
        "icon_emoji":":counteract:",
        "attachments":[
                {
                "fallback":"Peer to Peer Software Running",
                "color":"danger",
                "title":"Peer to Peer Software Running",
"title_link":"https://APPLIANCE_OR_EM/assets/rangesearch?main_selection=ip&query={ip}&address={ip}",
                "text":"P2P software is running on *{nbthost}*\n*OS:* {os_classification}\n*User:*
{user}\n*P2P Software:* {p2p_running}",
                }
]
}
]
}
```

As you can see the possibilities are very strong with how you can craft messages in slack. You can even create buttons in slack to perform actions. I have not finished the example below but you get the idea on the possibilities.



Forescout APP 7:42 PM

BOSMWR301XZ07 is Not Compliant with Full Disk Encryption. This device is connected to: 10.100.100.24:Gi10/31

What would you like to do

Frequently Asked Questions

After importing the Web Service Properties, they didn't map to the Web Service Requests. What gives?

For some of the integrations, they use a unique internal identifier that is different between Forescout environments. You just need to map them manually after importing.

Awesome integration! How can I contribute back?

First off, if you implemented this integration I want to know about it! Shoot me an email with your feedback. Second, I go through a lot of coffee while building these, so feel free to buy me a cup! paypal.me/NickDuda

Can you help me build an integration for <insert technology here>?

Absolutely! Hit me up at nduda78@gmail.com and let's chat.

Where can I go to learn more about all things Forescout?

- Forescout Slack User Community. - I'm a little biased on this one since I created it. This is probably the best place to go if you want realtime chat with Forescout experts (Customers, Partners and even Forescout Employees).
- Official Forescout Forum. - You'll need to be a customer to access it though. There is a good amount of activity going on there and the support team chimes in. This is, of course, the official Forescout method for asking questisons.
- Forescout on Reddit. - Not as active as the Slack Community or Forescout Forum but it's a place to get the attention of some experts.