



FORESCOUT®

Forescout and Microsoft Teams Integration

08.16.19 - v1.0

Nick Duda

nduda78@gmail.com

Twitter: [@nduda78](https://twitter.com/nduda78)

LinkedIn: <https://www.linkedin.com/in/nickduda/>

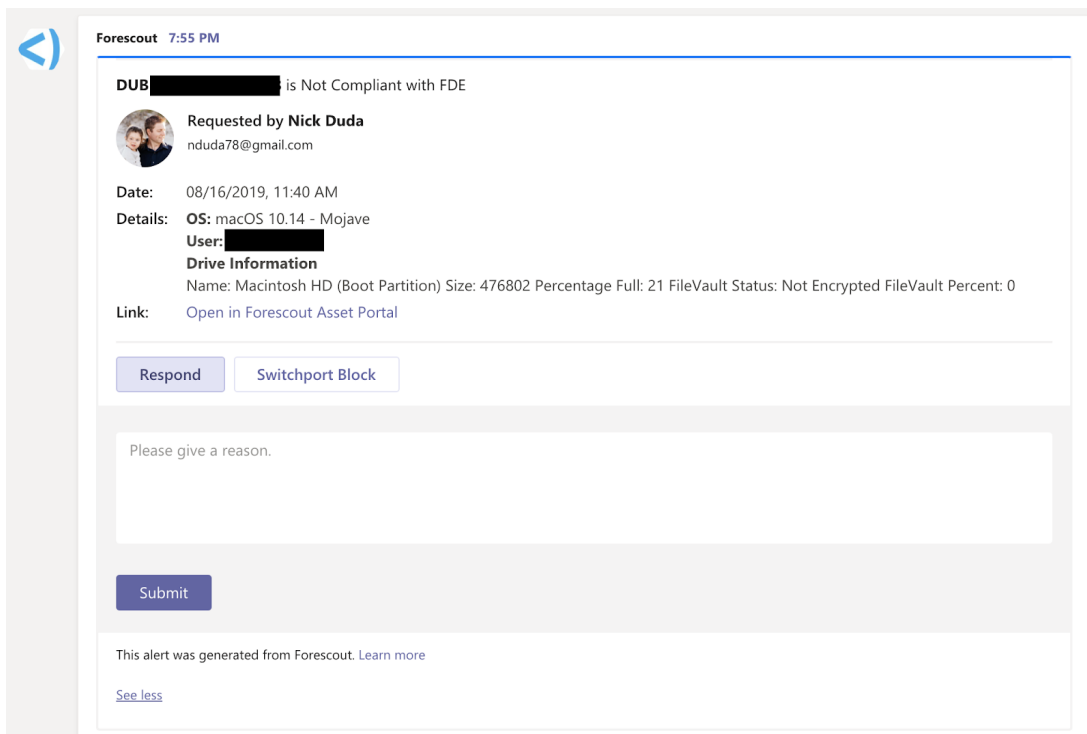
Summary

Using the Forescout Open Integrations Module (OIM), this document will walk you through integrating Forescout with Microsoft Teams. Teams is a unified communications platform that combines persistent workplace chat, video meetings, file storage (including collaboration on files), and application integration.

1. Post to a Team Channel


- a. Similar to the *Send Email* action, this action will post whatever you put in the json to the Team channel you pick.
- b. Based on the json options, you will be able to create posts with hyperlinks, message actions and more.

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 Teams you can immediately get alerted to policy triggers with hyperlinked actions in the channel post. Tags {tags} can be used in the json that posts into the channel as well.



The screenshot shows a Microsoft Teams chat window titled "Forescout 7:55 PM". The message content is as follows:

DUB [redacted] is Not Compliant with FDE

 **Requested by Nick Duda**
nduda78@gmail.com

Date: 08/16/2019, 11:40 AM
Details: OS: macOS 10.14 - Mojave
User: [redacted]
Drive Information
Name: Macintosh HD (Boot Partition) Size: 476802 Percentage Full: 21 FileVault Status: Not Encrypted FileVault Percent: 0

Link: [Open in Forescout Asset Portal](#)

Below the message are two buttons: "Respond" and "Switchport Block".

Below the buttons is a text input field with the placeholder text "Please give a reason."

Below the input field is a "Submit" button.

At the bottom of the chat window, there is a footer that reads: "This alert was generated from Forescout. [Learn more](#)" and a "See less" link.

In the example above, the post in the Forescout Team channel has passed through {tags} on a device not compliant with Full Disk Encryption including device name, user, OS and information on the disk drive. There is also a link that will bring you to the device in the Forescout Asset Portal. There is also an option to respond to the message (which will go to another team/user) and even the ability to perform actions (http posts)

Requirements

Forescout Requirements

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

Microsoft Team Requirements

1. A Microsoft Team Channel
 - a. You can sign up for a free Team account at <https://products.office.com/en-us/microsoft-teams/group-chat-software>
2. Building a Team channel incoming webhook for Forescout to post.

Configuration

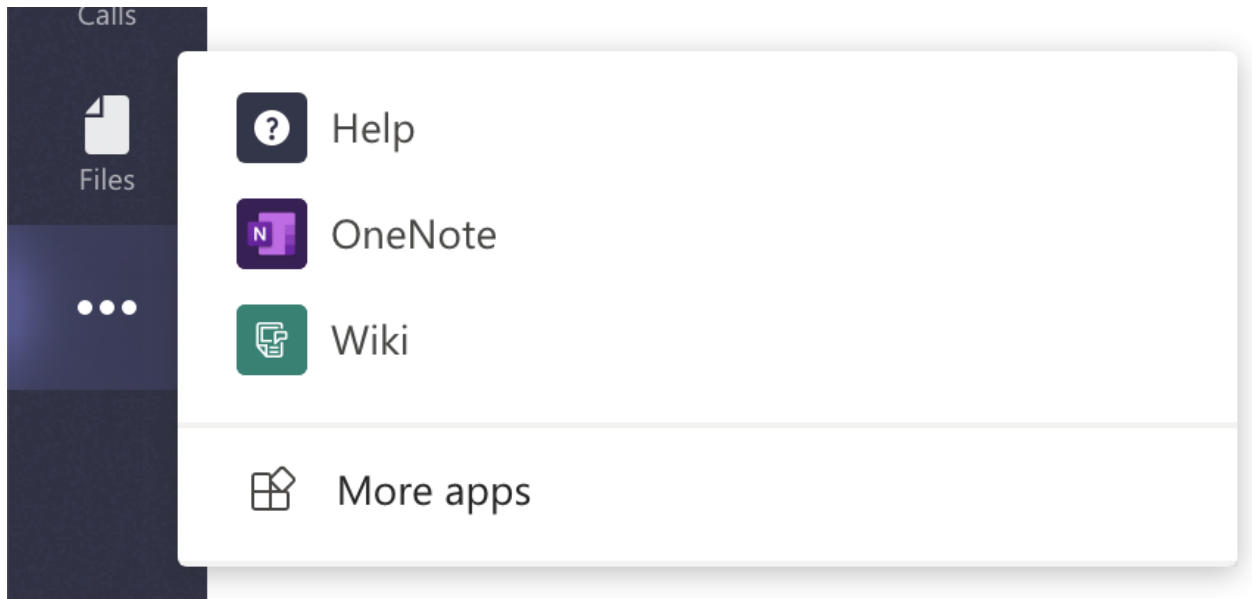
Creating a Microsoft Team Account

1. Navigate to <https://products.office.com/en-us/microsoft-teams/group-chat-software>
2. Sign-up for a Microsoft Team account

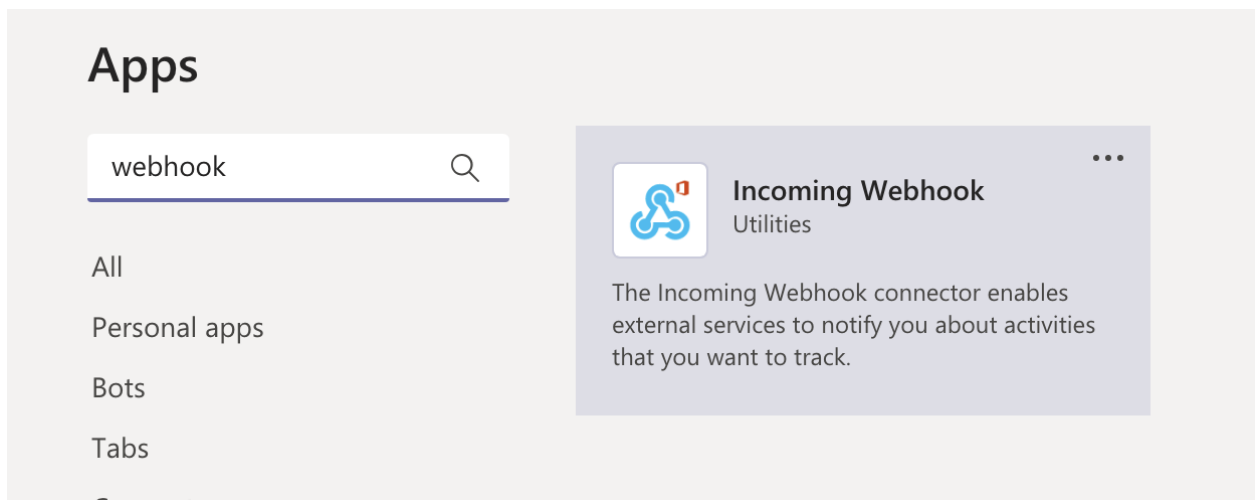
Creating the Incoming Webhook

1. Navigate and login to <https://products.office.com/en-us/microsoft-teams/group-chat-software>
 - a. You'll want to login to the Team account you want to integrate with.
2. Optional. Install the Team desktop client and work from within it. I found it easier to work with than the web UI.

3. From the sidebar, click the *triple dot icon* and select *More apps*



4. In the search bar type webhook. Click on Incoming Webhook and select install



5. Once the Incoming webhook app is installed you need to configure it.

- a. Add to a team. Select the Team you want to create the webhook for and click Open



Incoming Webhook



The Incoming Webhook connector enables external services to notify you about activities that you want to track.

► Add to a team

Forescout



Open

► About

► Privacy and permissions

By using Incoming Webhook, you accept its [privacy policy](#) and [terms of use](#):

6. Next, pick the channel within the Team you selected. Click Set up



Incoming Webhook is now available for Forescout



First, pick the channel where you want to use the app

General



Next, set up the features that you want



Connector

Get notifications right in a channel

Set up

- Next, give the Incoming Webhook a name. This is the name that will appear next to the posts in the Team Channel. Optional, Upload an Image. In this example I used the Forescout Logo. Click Create.

Connectors for "General" channel in "Forescout" team



Incoming Webhook

[Send feedback](#)

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the [Office 365 connector format](#).

Fields marked with * are mandatory

To set up an Incoming Webhook, provide a name and select Create. *

Customize the image to associate with the data from this Incoming Webhook.

Upload Image



Create

Cancel

- Once you click Create the Webhook URL is posted. **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.**

Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.

<https://outlook.office.com/webhook/995C>



Done

Remove

Create the action to post into the Microsoft Team Channel (webhook)

1. In the Forescout Console, navigate to the policy/sub-rule you want to perform the Team 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 Team channel this will post into.
 - b. HTTP Method: POST
 - c. Request URL: This is the Webhook URL from Step 8 in the last section.
 - d. HTTP message headers (raw): Content-Type: application/json
 - e. HTTP message body: This is where you will post the Team json that you want posted in the channel when the action is performed. To learn about all the options you can use in the json please see <https://docs.microsoft.com/en-us/outlook/actionable-messages/send-via-connectors>

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

Forescout 7:55 PM

DUB [redacted] is Not Compliant with FDE

Requested by Nick Duda
nduda78@gmail.com

Date: 08/16/2019, 11:40 AM

Details: OS: macOS 10.14 - Mojave
User: [redacted]

Drive Information
Name: Macintosh HD (Boot Partition) Size: 476802 Percentage Full: 21 FileVault Status: Not Encrypted FileVault Percent: 0

Link: [Open in Forescout Asset Portal](#)

[Respond](#) [Switchport Block](#)

Please give a reason.

[Submit](#)

This alert was generated from Forescout. [Learn more](#)

[See less](#)

```

{
  "@type": "MessageCard",
  "@context": "https://schema.org/extensions",
  "summary": "This is the summary property",
  "themeColor": "0075FF",
  "sections": [
    {
      "heroImage": {
        "image":
"https://www.forescout.com/wp-content/uploads/2018/01/forescout_logo_horizontal-color.png"
      }
    },
    {
      "startGroup": true,
      "title": "**{dhcp_hostname}** is Not Compliant with FDE",
      "activityImage":
"https://pbs.twimg.com/profile_images/899977555171790848/uHBRV6Ef.jpg",
      "activityTitle": "Requested by **Nick Duda**",
      "activitySubtitle": "nduda78@gmail.com",
      "facts": [
        {
          "name": "Date:",
          "value": ""
        },
        {
          "name": "Details:",
          "value": "**OS:** {os_classification}\n\n**User:**
{dexextweb_jamf_local_users}\n\n**Drive Information**\n\n{dexextweb_jamf_boot_device}"
        },
        {
          "name": "Link:",
          "value": "[Open in Forescout Asset
Portal](https://APPLIANCE_OR_EM/assets/rangesearch?main_selection=ip&query={ip}&address={ip})"
        }
      ]
    }
  ]
}

```



```

    }
  ]
},
{
  "potentialAction": [
    {
      "@type": "ActionCard",
      "name": "Respond",
      "inputs": [
        {
          "@type": "TextInput",
          "id": "comment",
          "isMultiline": true,
          "title": "Please give a reason."
        }
      ],
      "actions": [
        {
          "@type": "HttpPost",
          "name": "Submit",
          "target": "http://..."
        }
      ]
    }
  ],
  {
    "@type": "ActionCard",
    "name": "Switchport Block",
    "inputs": [
      {
        "@type": "TextInput",
        "id": "comment",
        "isMultiline": true,

```

```

        "title": "Reason (optional)"
      }
    ],
    "actions": [
      {
        "@type": "HttpPost",
        "name": "Submit",
        "target": "http://..."
      }
    ]
  }
}
},
{
  "startGroup": true,
  "activitySubtitle": "This alert was generated from Forescout. [Learn
more](https://some_url)\n\n"
}
]
}

```

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](https://www.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 questions.
- [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.