

**Aon Inpoint ClaimsMonitor application and Okta
SCIM Integration Guide**

Table of Contents

1 Overview	3
2 Support features	3
3 Supported SCIM Attributes.....	3
4 Requirements.....	3
5 Configuration Steps	3
6 Known Issues/Troubleshooting.....	6

1 Overview

This guide provides the steps required to configure Provisioning for **Aon Inpoint ClaimsMonitor** application (short name: **ClaimsMonitor**) in Okta.

2 Support features

The following provisioning features are supported by **ClaimsMonitor** at present:

- **Create Users:** users in Okta that are assigned to the **ClaimsMonitor** within Okta are automatically added as users in **ClaimsMonitor**
- **Update User Attributes:** when user attributes are updated in Okta, they will be updated in **ClaimsMonitor**
- **Deactivate Users:** when users are deactivated in Okta, they will be set to “inactive” within **ClaimsMonitor**, which prevents the user from logging into **ClaimsMonitor**

3 Supported SCIM Attributes

- `userName` – *email address*
- `givenName`
- `familyName`
- `primaryPhone`

4 Requirements

Before configuring the user provisioning for **ClaimsMonitor**, you must reach out to the [Aon Inpoint support](#) to activate the feature. The following items will be provided:

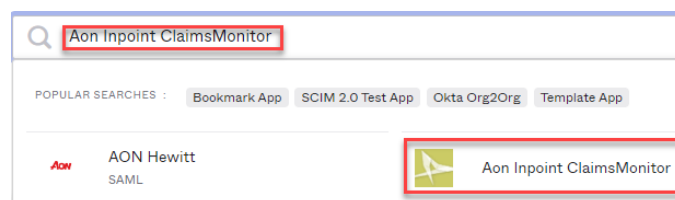
- SCIM 2.0 Base Url
- OAuth Bearer Token

5 Configuration Steps

1. Install Application

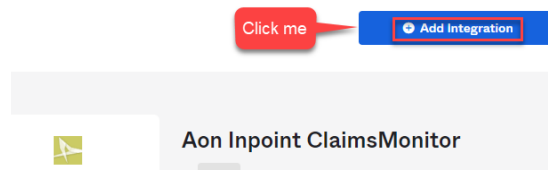
If you already have **Aon Inpoint ClaimsMonitor** as an application, **click on it**, otherwise installing the application by following the four steps below.

1.1 Click “Applications” > “Applications” > “Browse App Catalog”

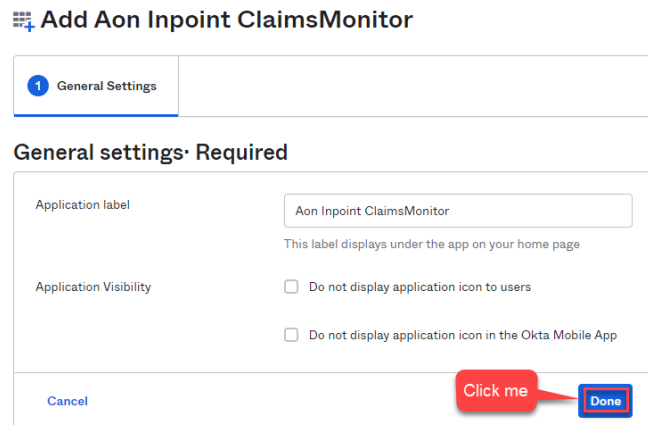


1.2 Enter **Aon Inpoint ClaimsMonitor** in the search box

1.3 Click the searched app  which opening the **Add Integration** page



1.4 Click **“Add Integration”** button, it will open the Add **Aon Inpoint ClaimsMonitor** page as follows, then click **Done** button



2. Configure Integration and To App attributes

2.1 Navigate to the **Provisioning** tab and then click **Configure API Integration**

Provisioning is not enabled
Enable provisioning to automate Aon Inpoint ClaimsMonitor user account creation, deactivation, and updates.

[Configure API Integration](#)

2.2 Check the **“Enable API Integration”**, and then enter the SCIM 2.0 Base Url and OAuth Bearer Token provided by the [Aon Inpoint support](#)

Enable API integration

Enter your Aon Inpoint ClaimsMonitor credentials to enable user import and provisioning features.

Base URL

API Token

[Test API Credentials](#)

[Save](#)

2.3 Click the [Test API Credentials](#) button to ensure the integration can connect successfully, and then click the [Save](#) button upon the completion of step#3.3, in the **Settings** panel, the **“To App”** option should be appeared.

2.4 Click the **“To App”** link, the Provisioning to App page appears. Click the Edit button, then check the “Enable” checkbox for the Create Users, Update User Attributes, and Deactivate Users











The screenshot shows the 'Provisioning to App' configuration page. On the left, a sidebar menu has 'To App' highlighted. The main content area shows the 'Provisioning to App' title and a 'Cancel' button. Below are four sections, each with a title, a description, and an 'Enable' checkbox:

- Create Users**: Description: 'Creates or links a user in SCIM 2.0 Test App (OAuth Bearer Token) when assigning the app to a user in Okta. The default username used to create accounts is set to Email.' The 'Enable' checkbox is checked and highlighted with a red box.
- Update User Attributes**: Description: 'Okta updates a user's attributes in SCIM 2.0 Test App (OAuth Bearer Token) when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SCIM 2.0 Test App (OAuth Bearer Token).' The 'Enable' checkbox is checked and highlighted with a red box.
- Deactivate Users**: Description: 'Deactivates a user's SCIM 2.0 Test App (OAuth Bearer Token) account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.' The 'Enable' checkbox is checked and highlighted with a red box.
- Sync Password**: Description: 'Creates a SCIM 2.0 Test App (OAuth Bearer Token) password for each assigned user and pushes it to SCIM 2.0 Test App (OAuth Bearer Token).' The 'Enable' checkbox is unchecked.

A 'Save' button is located at the bottom right of the page.

2.5 Click the [Save](#) button to save the changes above

2.6 After **step#2.5**, scroll a bit down, there is a section “Aon Inpoint ClaimsMonitor User Attribute Mappings”, **confirm** all the following attributes are mapped

Attribute	Attribute Type	Value	Apply on
Username userName	Personal	Configured in Sign On settings	
Given name givenName	Personal	user.firstName	Create and update  
Family name familyName	Personal	user.lastName	Create and update  
Email email	Personal	user.email	Create and update  
Primary email type emailType	Personal	(user.email != null && user.email != "") ? 'work' : "	Create and update  
Primary phone primaryPhone	Personal	user.primaryPhone	Create and update  
Hide Unmapped Attributes			

3. **Navigate to Credentials Details** in the tab **Sign On > Settings**, ensure that the value “**Email**” is selected as the Application username format, *if not editing the **Settings** page, and select the correct value, and save.*

Credentials Details

Application username format

Update application username on

Create and update

4. **Select** users to be Provisioned in **ClaimsMonitor**

The **Assignments** tab will let you provision your Okta users to **ClaimsMonitor**.

On the **Assignments** tab

4.1 Select “Assign” > “Assign to Groups” (*You can optionally select Assign to People*)

4.2 Click “Assign” next to any group(s) and then click “Done”

6 Known Issues/Troubleshooting

- Changing the **Primary Email Address** to be a different value with **username** won’t take effect as our application considers both attributes are identical
- The **username** must be unique across all tenants