Multi-Org Security Summary

Gain insight into Salesforce security settings across your company!

Installation Guide (for v2.7 - August 2020)

Introducing Multi-Org Security Summary

Complete insight into the security health of orgs across your company

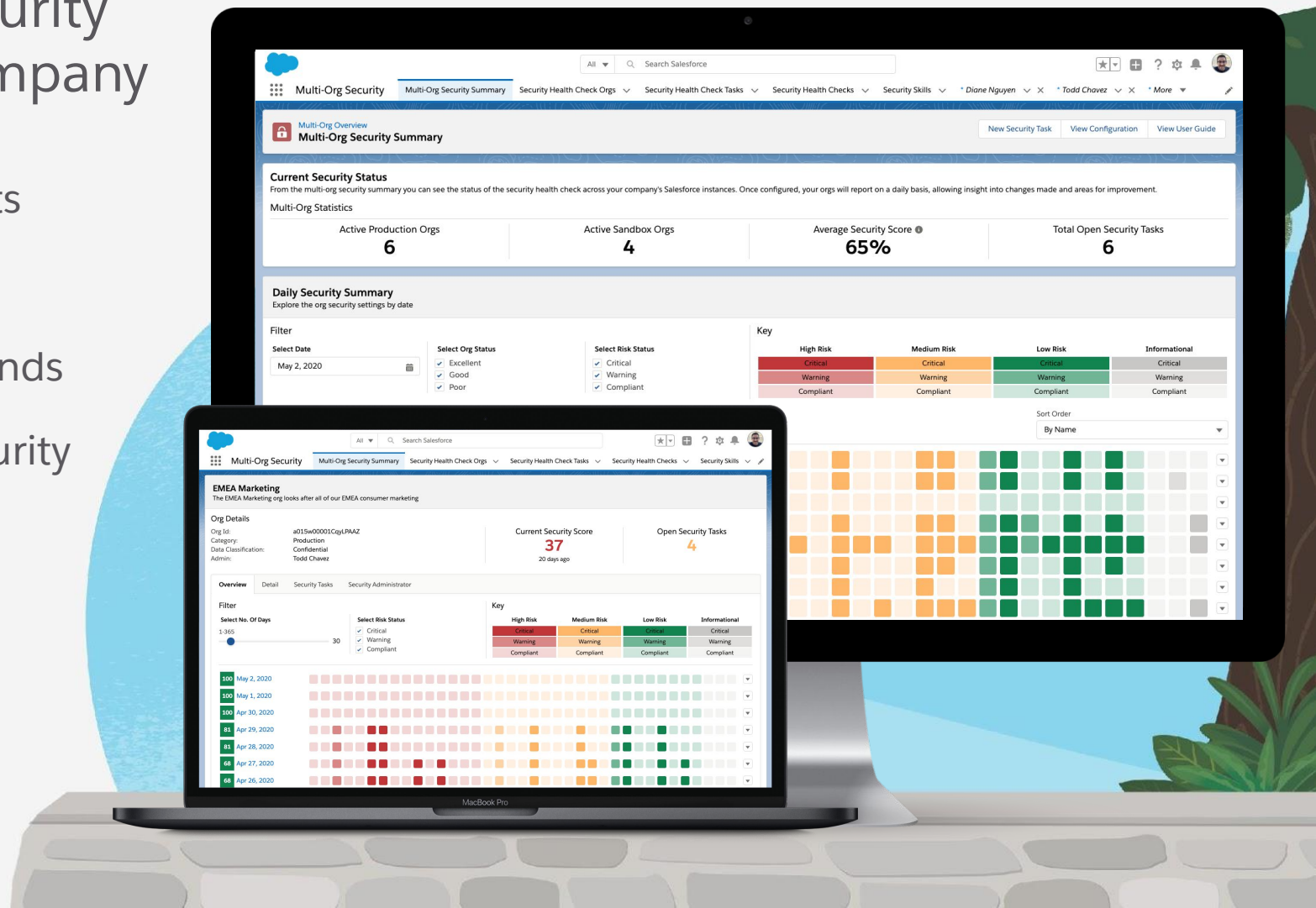
Powered by Lightning Web Components

Easy to install and simple to configure

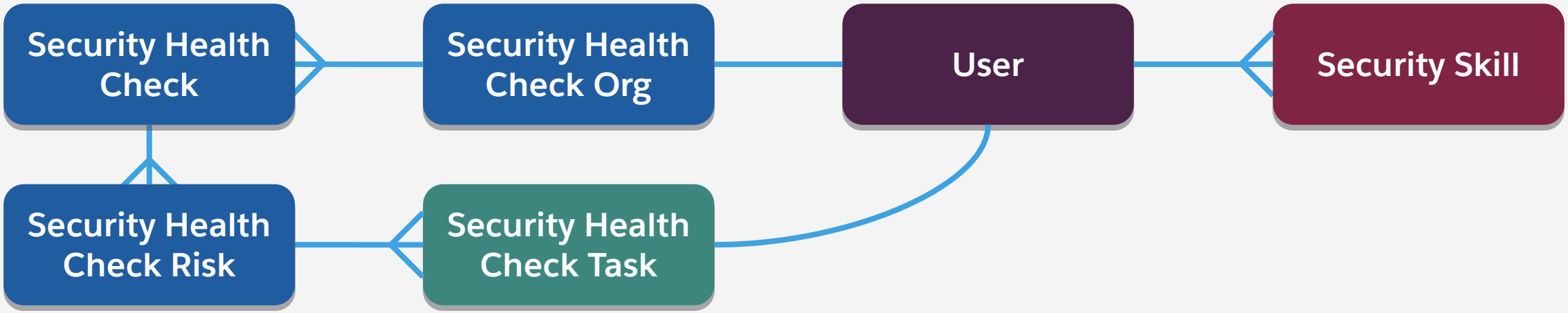
Access to scores, risks and historical trends

Create and assign tasks to improve security

100% natively built on Salesforce



Core Object Model



Security Health Check - A daily snapshot of a Salesforce orgs security health check and associated risks.

Security Health Check Org - The definition of the org that is connected to a security health check.

Security Health Check Task - A task used to instruct users when security risks need to be mitigated.

Security Skill - A record of your Admin's skills and commitment to learning.

Multi-Org Security Summary

Set up the central org by creating a record for each of your orgs.

Install the package into each child org and enter the required configuration.

Schedule the reporting service, which will report daily data to the central org.

Use the Multi Org Security app to view the summary of this data.

Each day will contain the security score and associated risk information.

Review the risks, paying particular attention to those marked Critical.

Identify orgs or risks that need to be reviewed and improved.

Assign tasks to the relevant admin, with an appropriate deadline and priority.

See the result of changes as your org scores improve.

Setup Guide

Configuration Instructions

Start by installing the package in the **central** org. This org will be the one that collates data across all of your orgs. Once installed you will need to perform the following actions

1. Open the *Multi-Org Security* app via the app launcher

2. Open the *Security Health Check Orgs* tab and click *New* to create the org record for the Central org. This is needed so that details about the central org can appear in the summary pages. [See the next page for details of what to provide]

Setting up the Central Org

Security Health Check Org

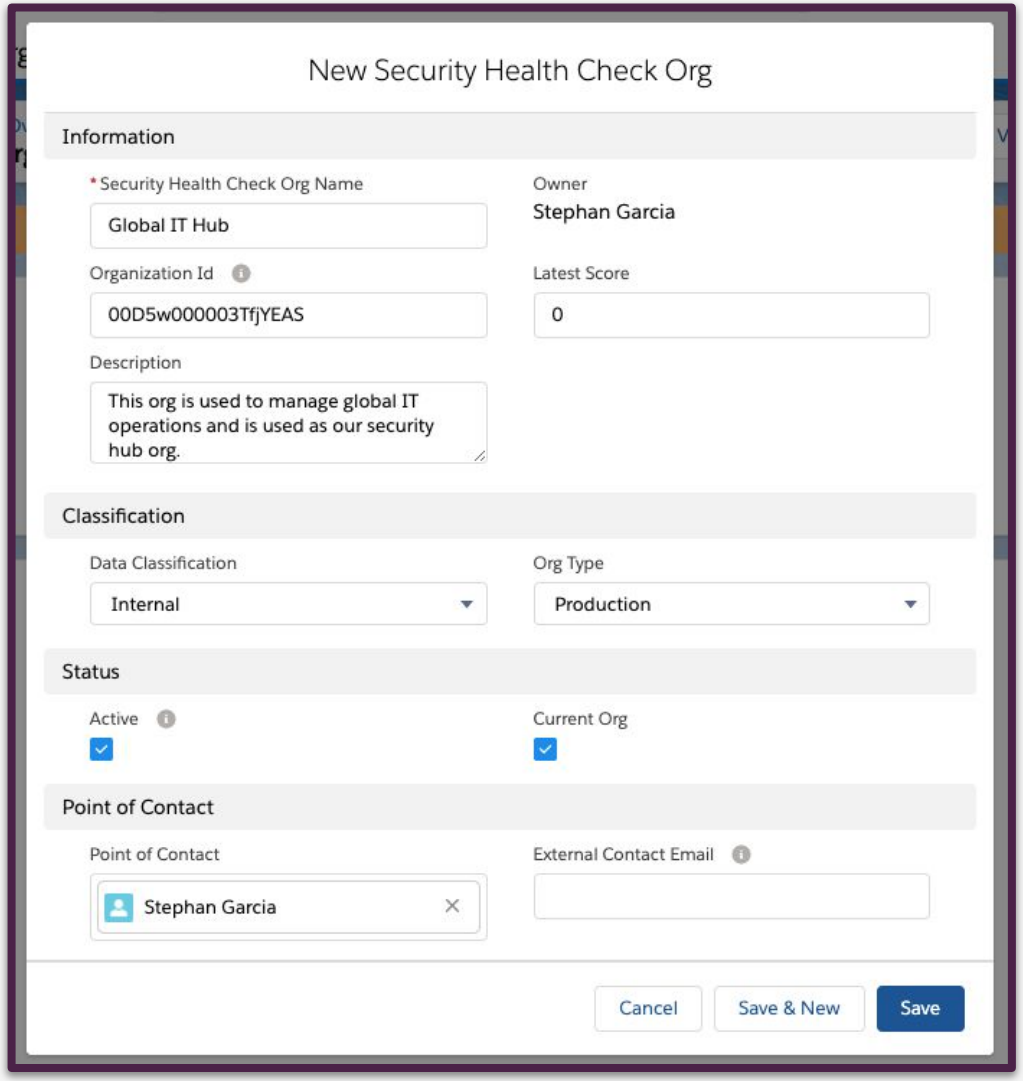
The security health check org record is used categorize and store security health checks against the relevant org.

Name: The name of the central Org

Organization Id: The Id of the central Org. This can be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org



Setting up the Central Org

Security Health Check Org cont.

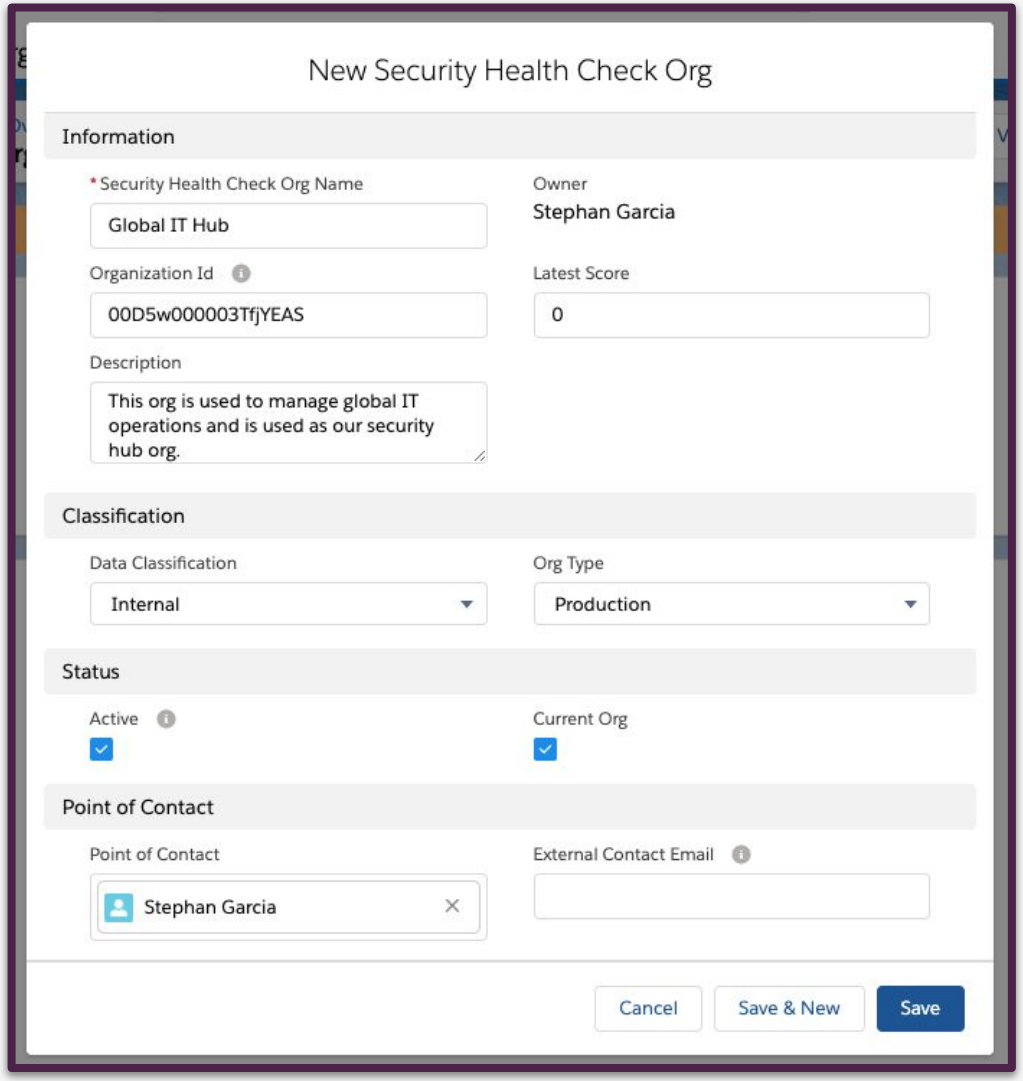
Org Type: Production or Sandbox

Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to true

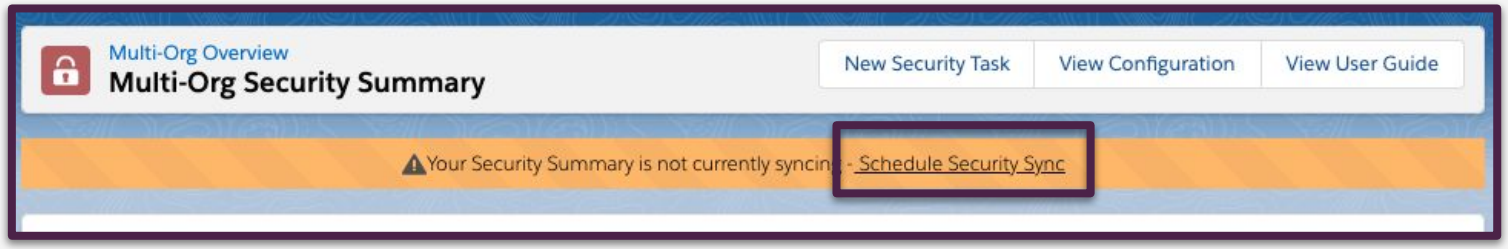
Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org



Schedule your Health Check Sync

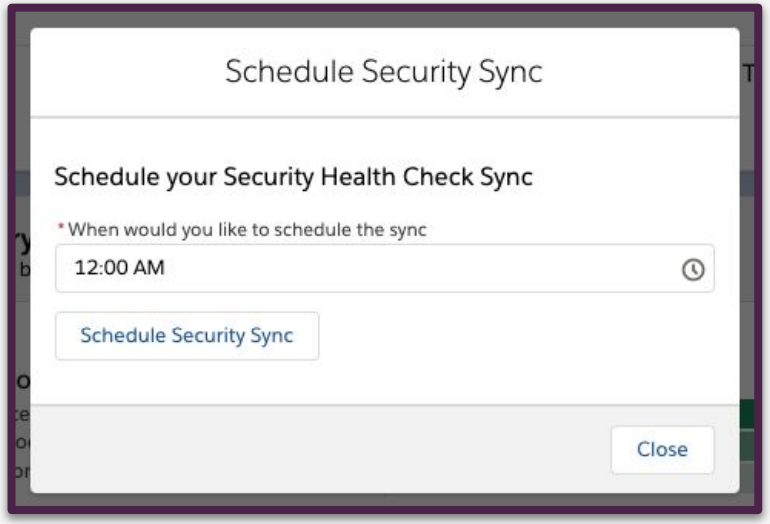
3 Navigate back to the Multi-Org Security Summary tab and you will see the following banner displayed on the page.



4 Select *Schedule Security Sync* and follow the instructions. This will generate your first set of data for this org.

At the next prompt, select the time of day to schedule the daily data generation and click *Schedule Security Sync*. [Ideally this should be set up to be around the same time for this central org and all other child orgs].

5 After the job has been scheduled, close the prompt and refresh the page. You should now see the daily security summary with your central org listed and data populated.



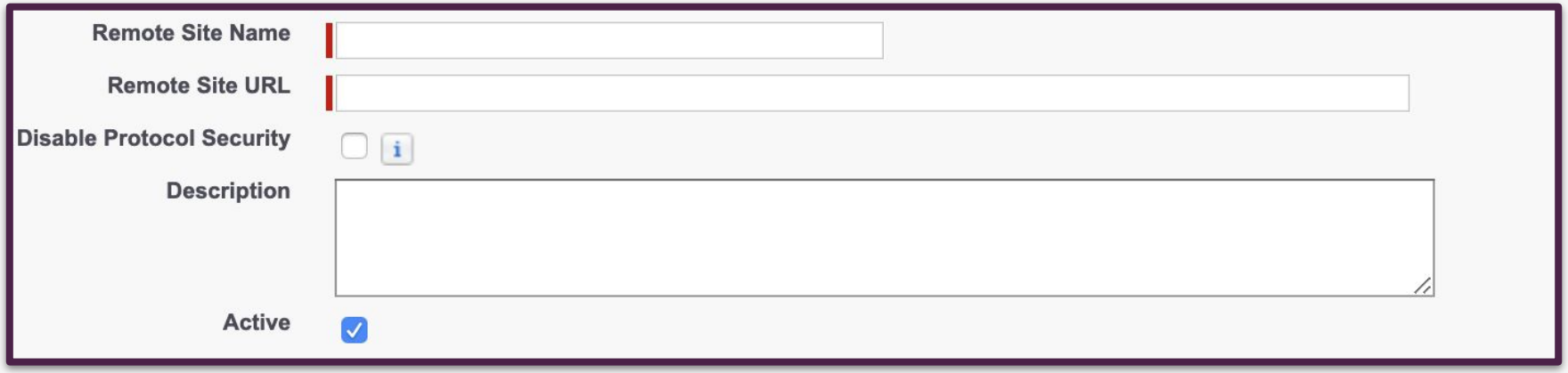
Create the Reporting Endpoint

Create Remote Site Settings

Create A Remote Site Settings in the Central Org

Navigate to *Setup* > *Remote Site Settings*

6 **Create Remote Site Setting:** https://**this-org-mydomain**--c.visualforce.com
This link for the central org will allow us to get the Health Check from the Tooling API



Choose your Integration Method

The security health checks are sent to this central org via a HTTP POST request. There are two options around how to configure the endpoint that receives the data :-

OPTION 1

Salesforce Rest Api & Connected App

Create a connected app and authorize each of your child orgs to communicate with Salesforce.

Then use an Authorization provider and named credential in the child org to send the security health check data to the central org.

OPTION 2

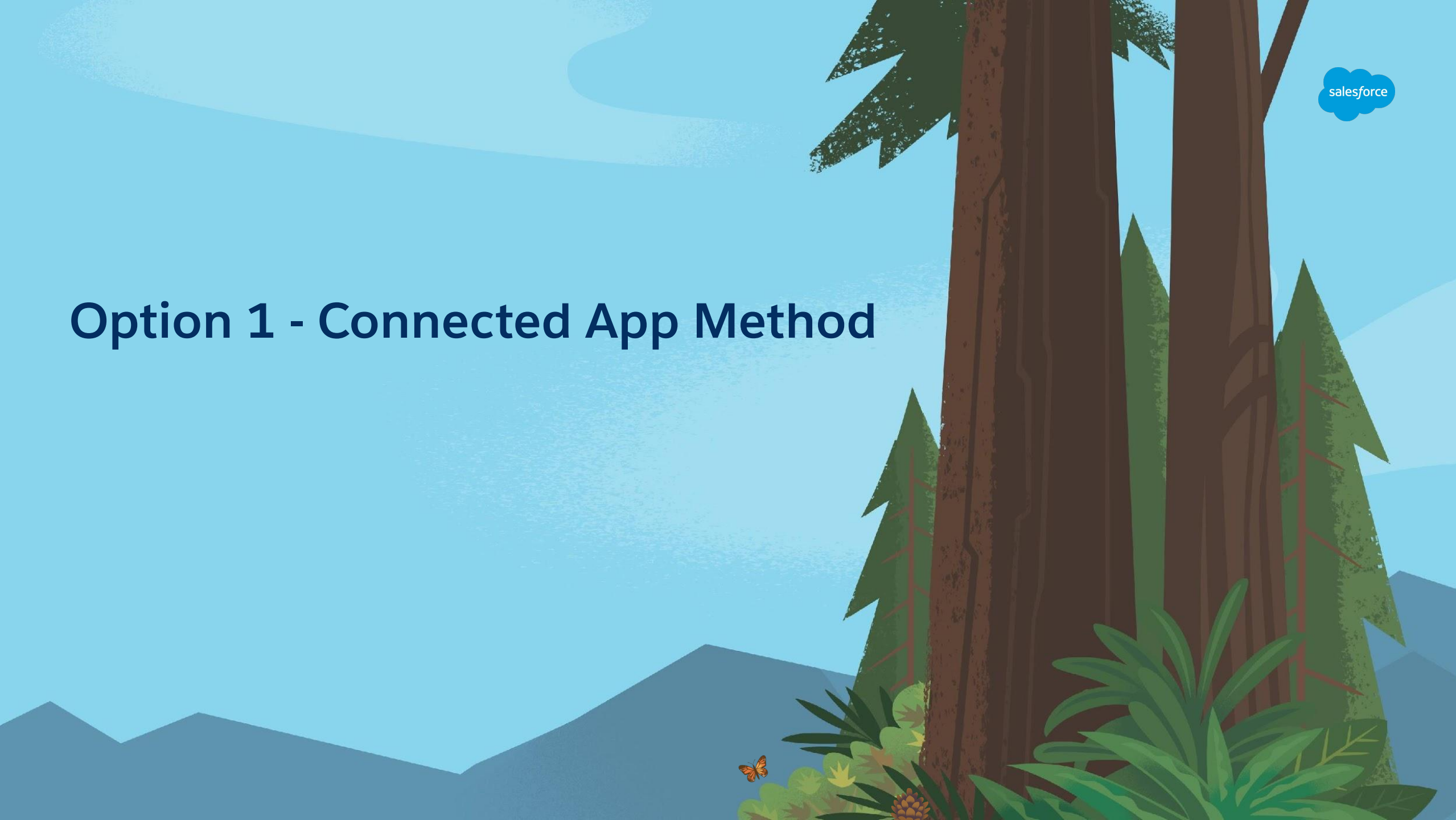
Public Salesforce Site Endpoint

Create a public salesforce site and add the supplied Apex Rest service to the site.

Once added, you may add the url of the endpoint to the child org and post the security health check data.

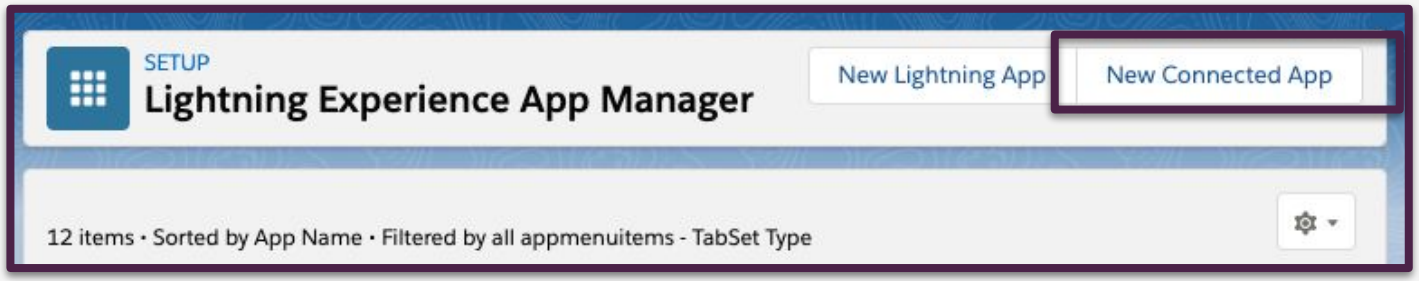
Choose ONE of these methods. The approach with the least amount of administration is OPTION 2.

Option 1 - Connected App Method



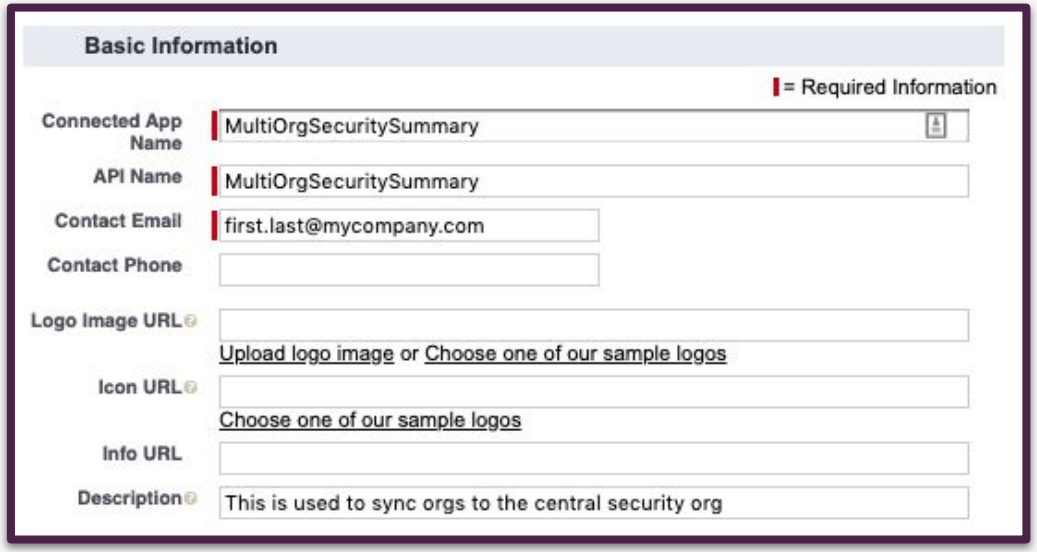
Option 1- Connected App Method (1/3)

7 Navigate to Setup > App Manager and Select ‘New Connected App’



8 Complete the basic information section of the app.

Make sure you give it a name that is recognizable to yourself and other administrators.

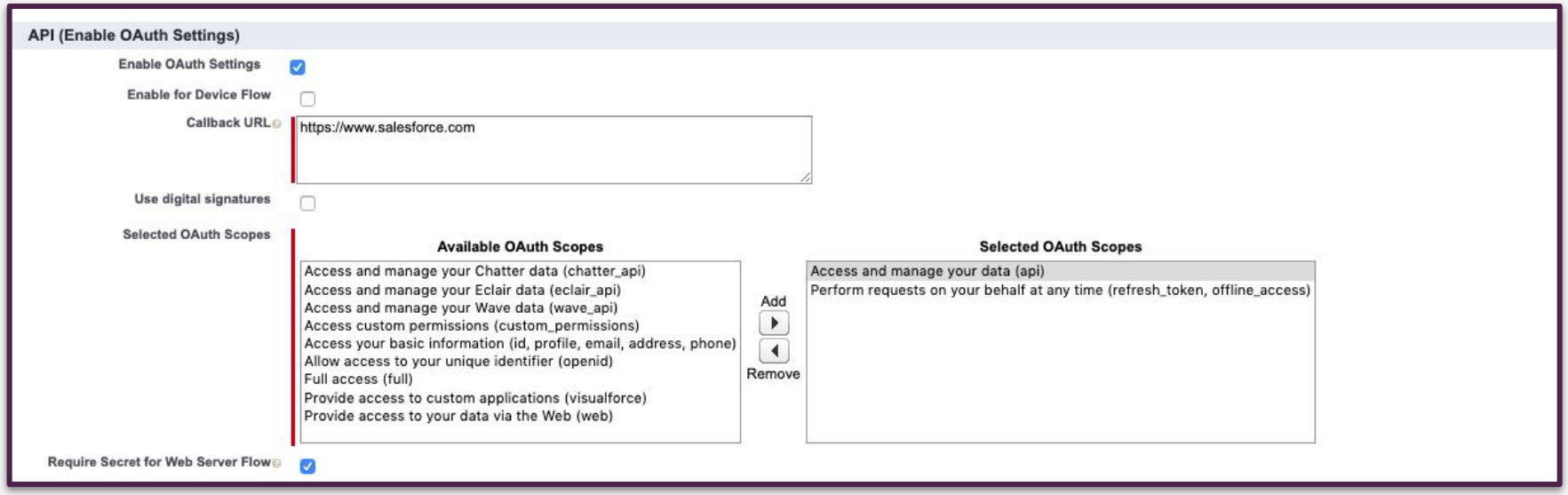


Option 1- Connected App Method (2/3)

9 Enable **OAuth Settings** and Supply a Temporary Callback URL [*the actual URL will be updated later after we have configured the child org*].

The application then requires you to Select the **refresh_token** and api **OAuth Scopes**

10 **Save your connected App**



Option 1- Connected App Method (3/3)

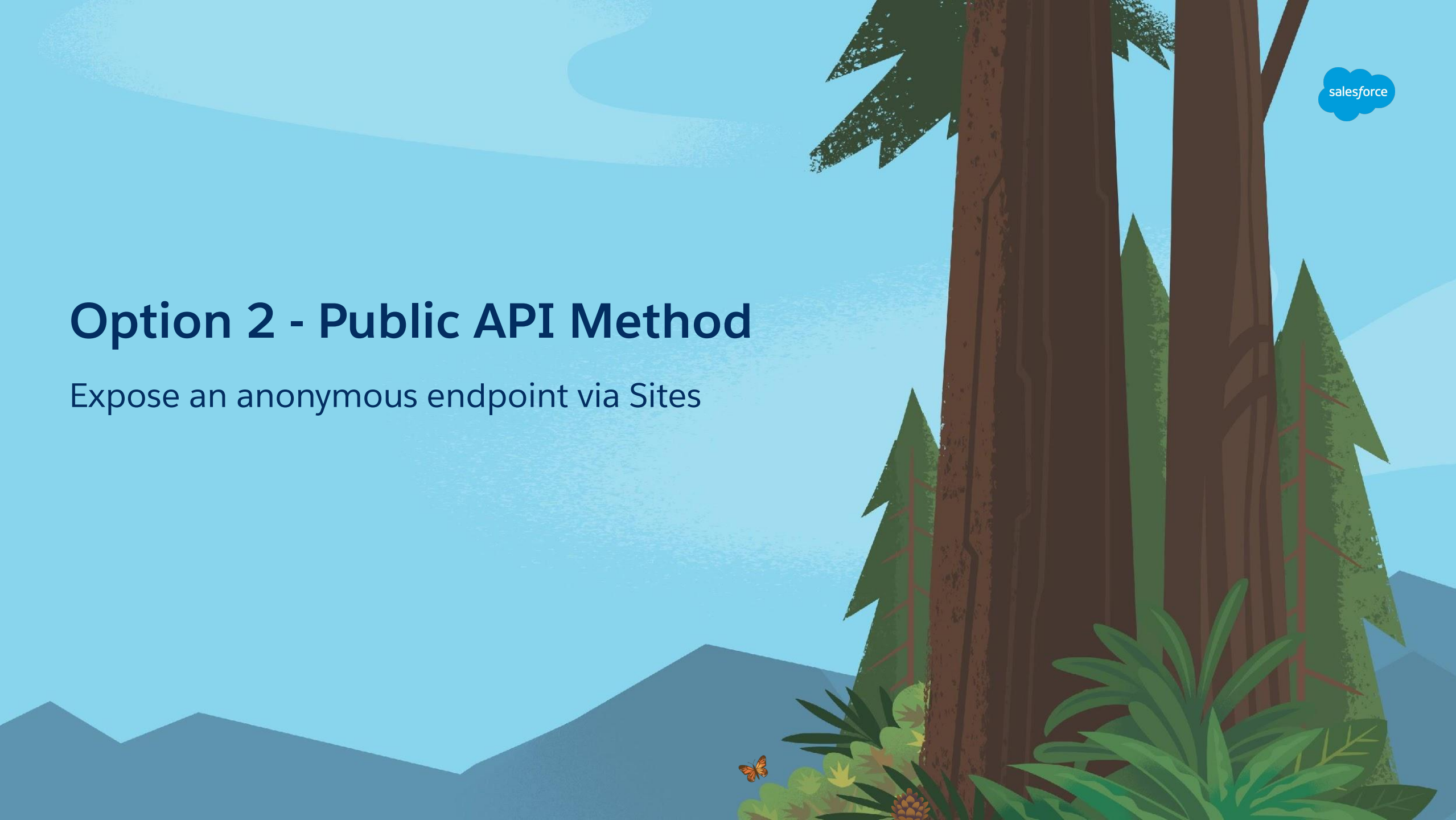
11 Navigate to *Setup* > *Profiles* and locate the profile of the user you will be using with the connected app

Select the Profile and then navigate to *Assigned Connected Apps*. Click ‘Edit’ and give them access to the connected App you just created. This is required so that the Named Credentials in the child org are able to connect. **If you do not do this you will receive an OAUTH_APP_ACCESS_DENIED error when authenticating later.**

12 **Save the Profile**

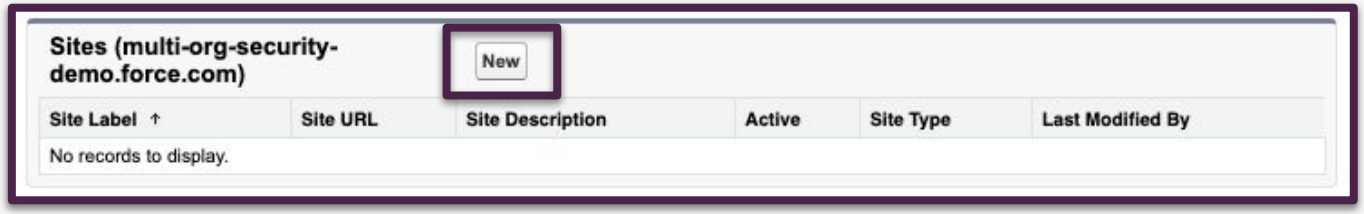
Option 2 - Public API Method

Expose an anonymous endpoint via Sites



Option 2 - Salesforce Sites Method

13 Navigate to Setup > Sites and Select ‘New’

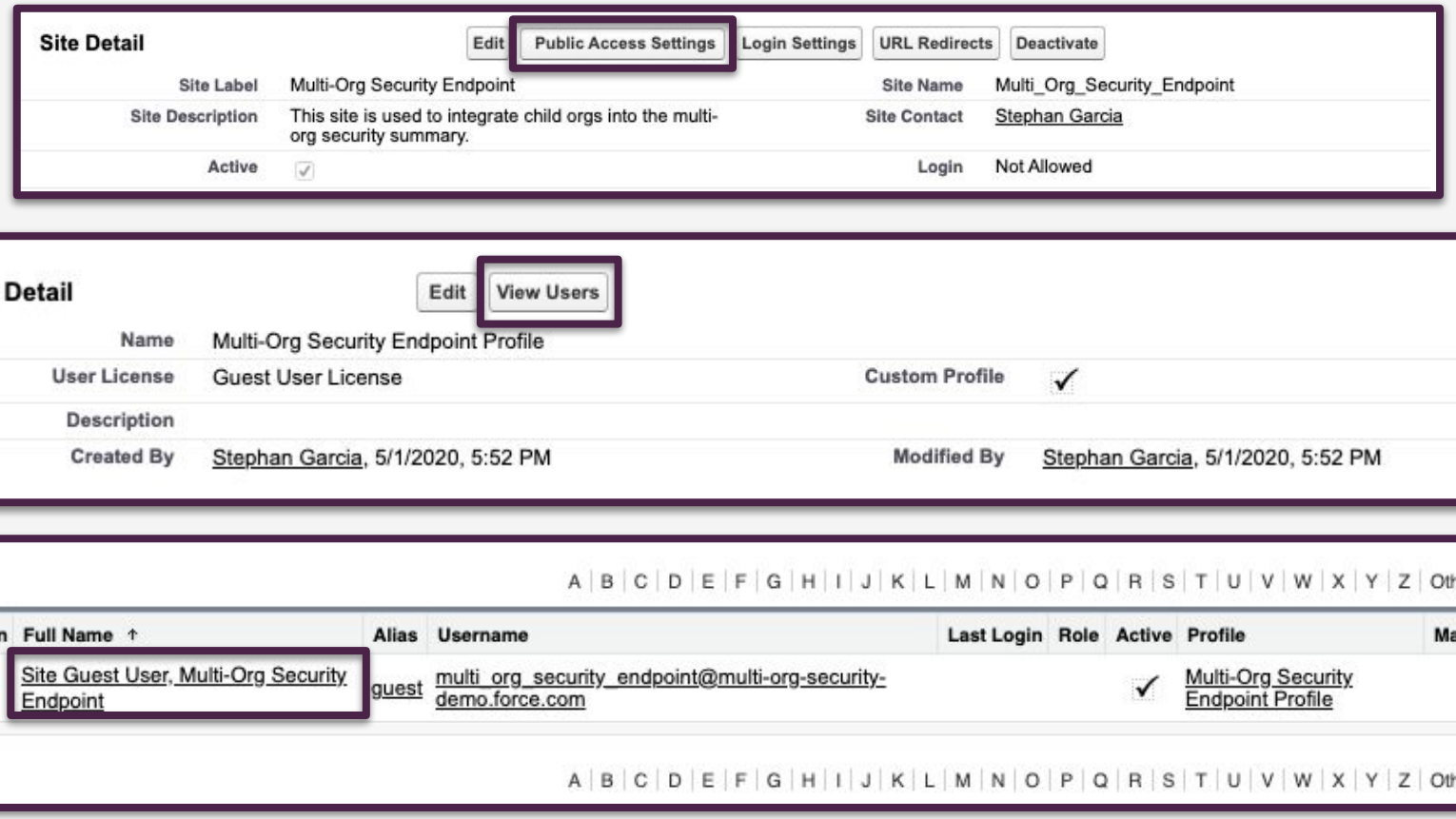


14 Select ‘Guest User Licence’ , Complete the basic information section and complete the security section in line with your company security policies. Remember to tick ACTIVE to make the site live.

Option 2: Salesforce Sites Method (cont.)

15

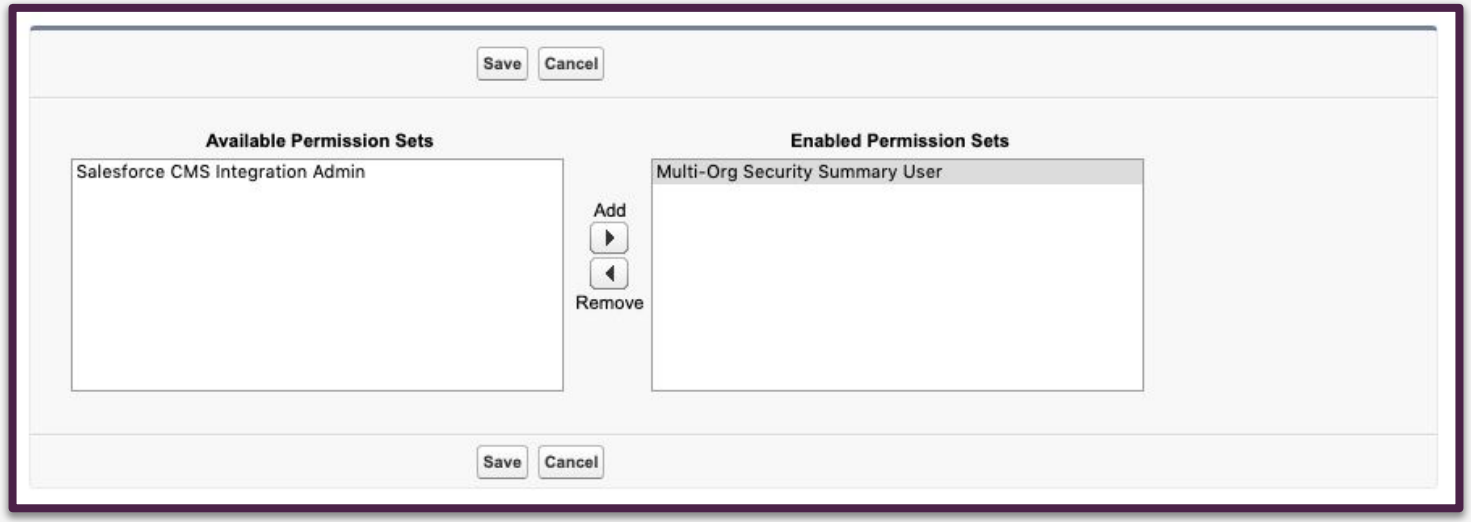
Once the site has been created - Select Public Access Settings > Assigned Users > Public Site User Full Name



Option 2: Salesforce Sites Method (cont.)

16

On the user profile, give the user the permission set ‘Multi-Org Security Summary Integration User’. This will give them access to the rest endpoint that allows them to POST their security health check securely.



Once this is completed - we will come back later when it’s time to integrate the child org.

Finalise the Central Org Configuration

The following instructions apply regardless of whether you are using Option 1 or Option 2.

Central Org - Metadata configuration (1/2)

17 Clone the Security Health Check Config

Navigate to *Setup > Custom Metadata Types*

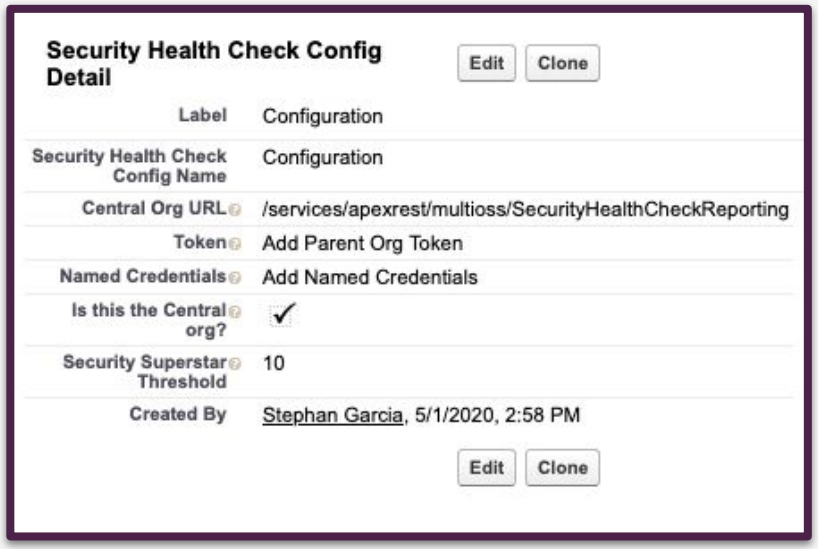
Select *Manage Records* for the Security Health Check Config record and then select *Configuration* in the configs list.

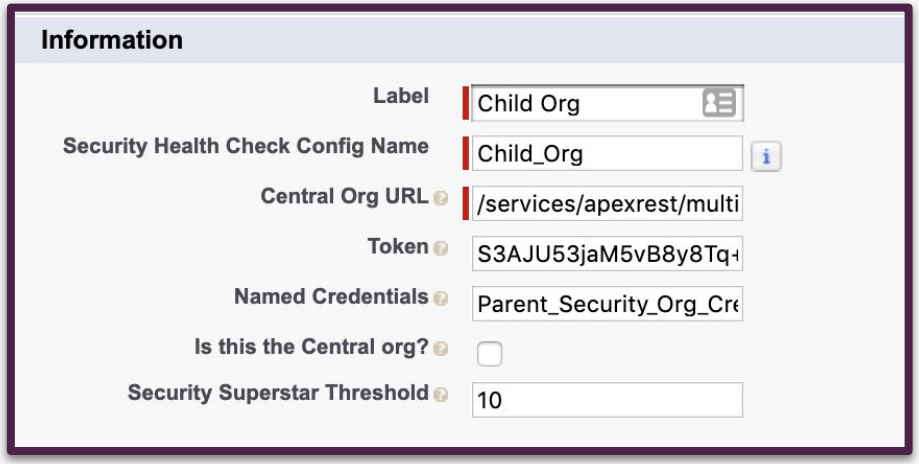
Clone the record.

Label: Give this a label that allows you to identify the record

Security Health Check Config Name: Make sure you change this to reflect the Label above. *[If the Name is left as Configuration, it will be ignored]*

Central Org URL: Leave as the default





[continue on the next page]

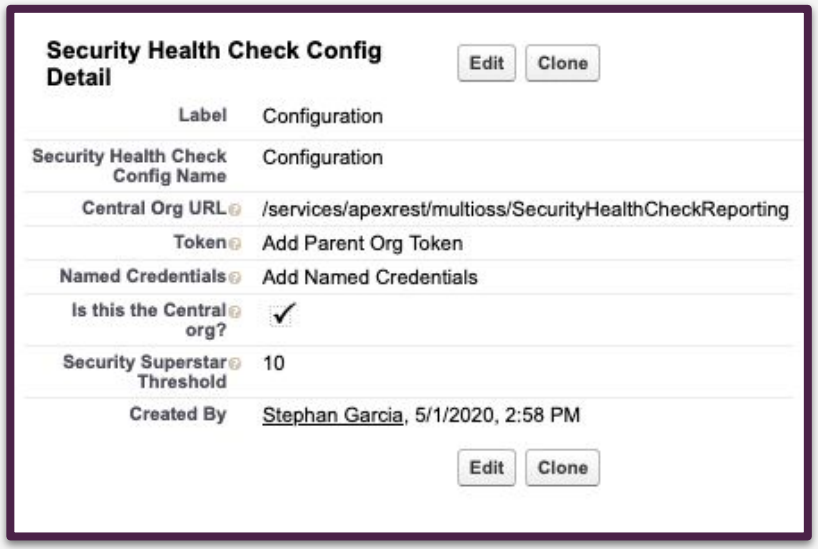
Central Org - Metadata configuration (2/2)

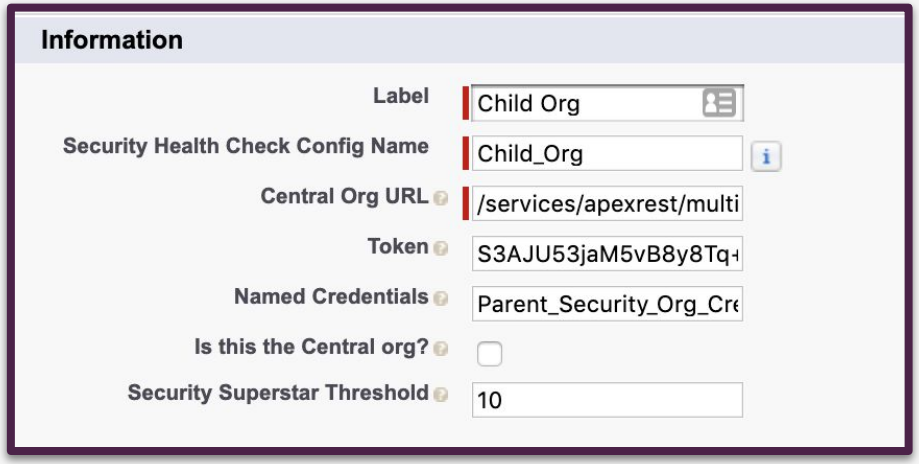
Token: This is not needed in the central org, so leave as is

Named Credentials: This is not needed, so leave as is

Is this the central org: True. This setting controls whether you see the multi-org version of the app page, or the single org version.

18 **Save** the record



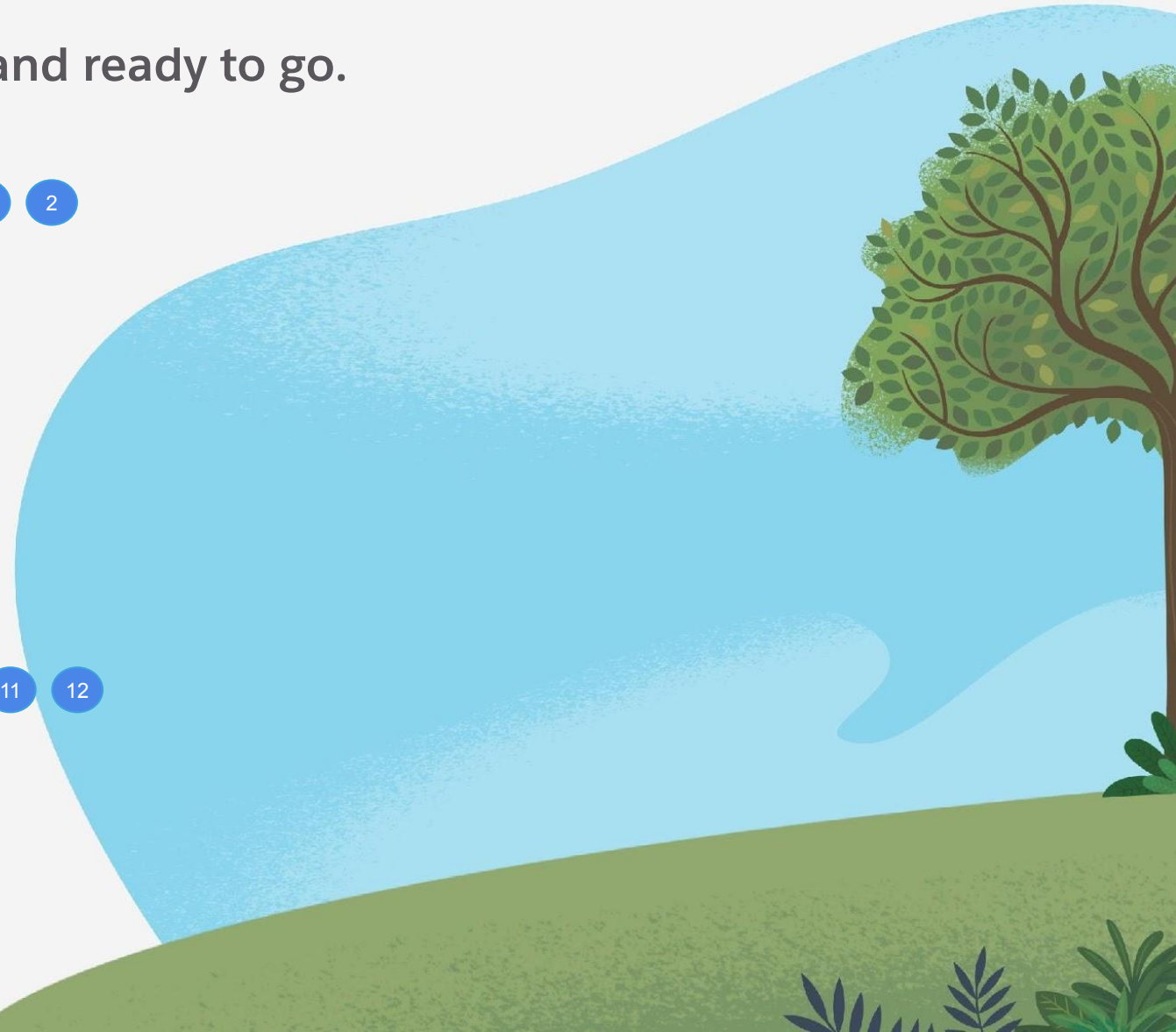


Central Org Checklist

That should be the central org configured and ready to go.
Ensure that you have:-

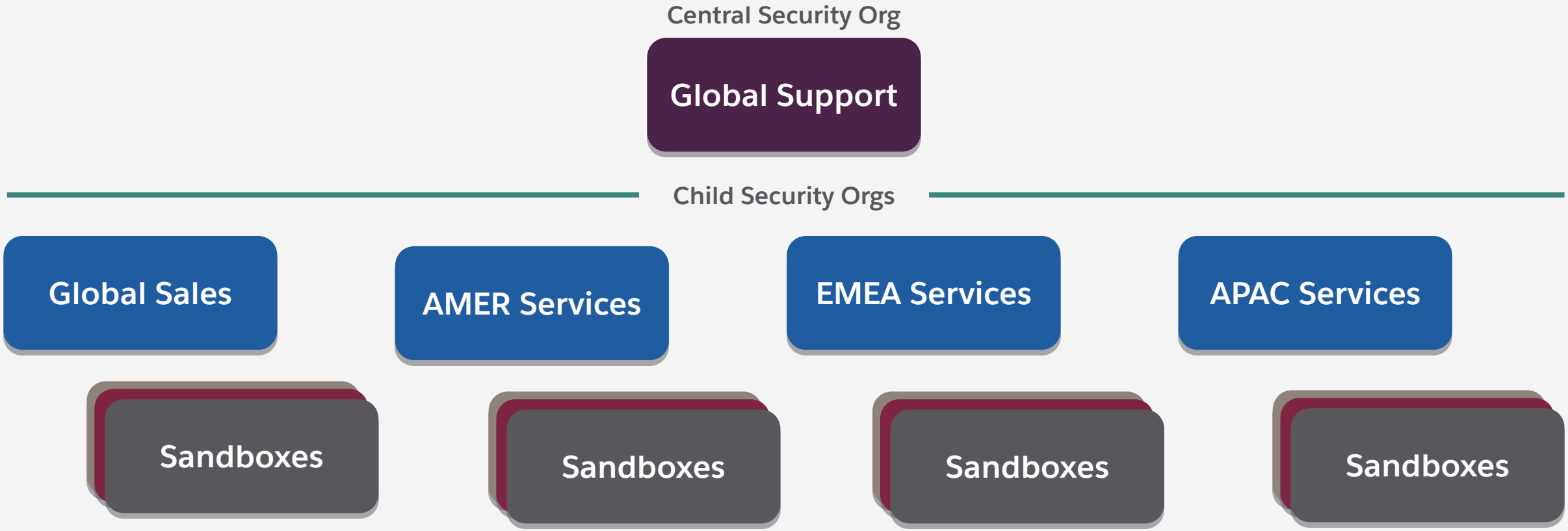
- Created a Security Health Check Org 1 2
- Scheduled the sync job 3 4 5
- Created a Remote Site Setting 6
- Set up the api endpoint
  - Connected App Method 7 8 9 10 11 12

    OR
  - Public Site Method 13 14 15 16
- Cloned the metadata type 17 18



Multi-Org Security Reporting

Once a main security org is designated - each of your child orgs can be configured to send their daily security health checks to the central org



Setting up the Child Orgs

Repeat these steps for each child org.....

Set Up The Central Configuration

Start by creating an entry in the **central** org. This is needed so that the data received can be grouped against the relevant org.

1. Open the *Multi-Org Security* app via the app launcher

2. Open the *Security Health Check Orgs* tab and click *New* to create the org record for this child org. [See the next page for details of what to provide]

Create Central Security Health Check Record (1/3)

Security Health Check Org

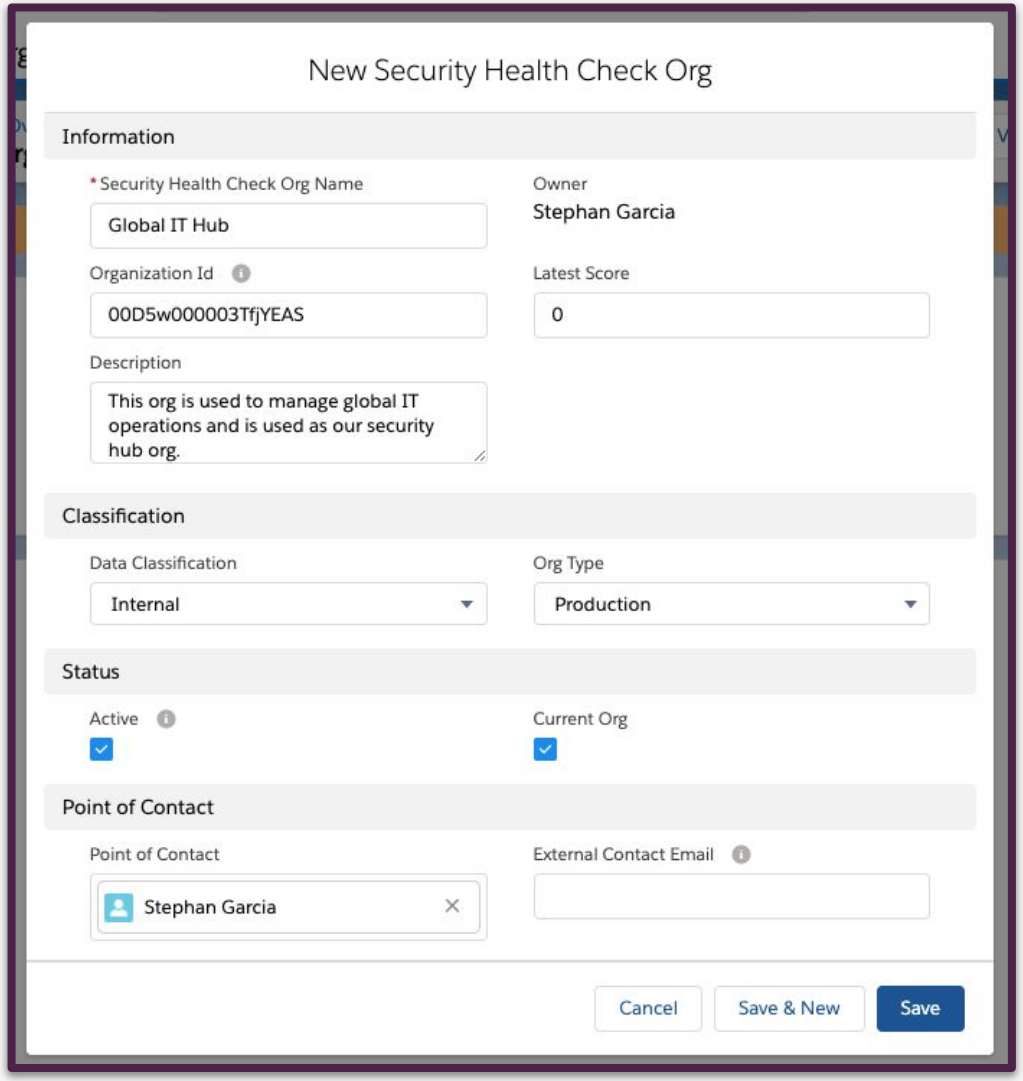
The security health check org record is used categorize and store security health checks against the relevant org.

Name: The name of the Org

Organization Id: The Id of the Org. This can be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org



Create Central Security Health Check Record (2/3)

Security Health Check Org cont.

Org Type: Production or Sandbox

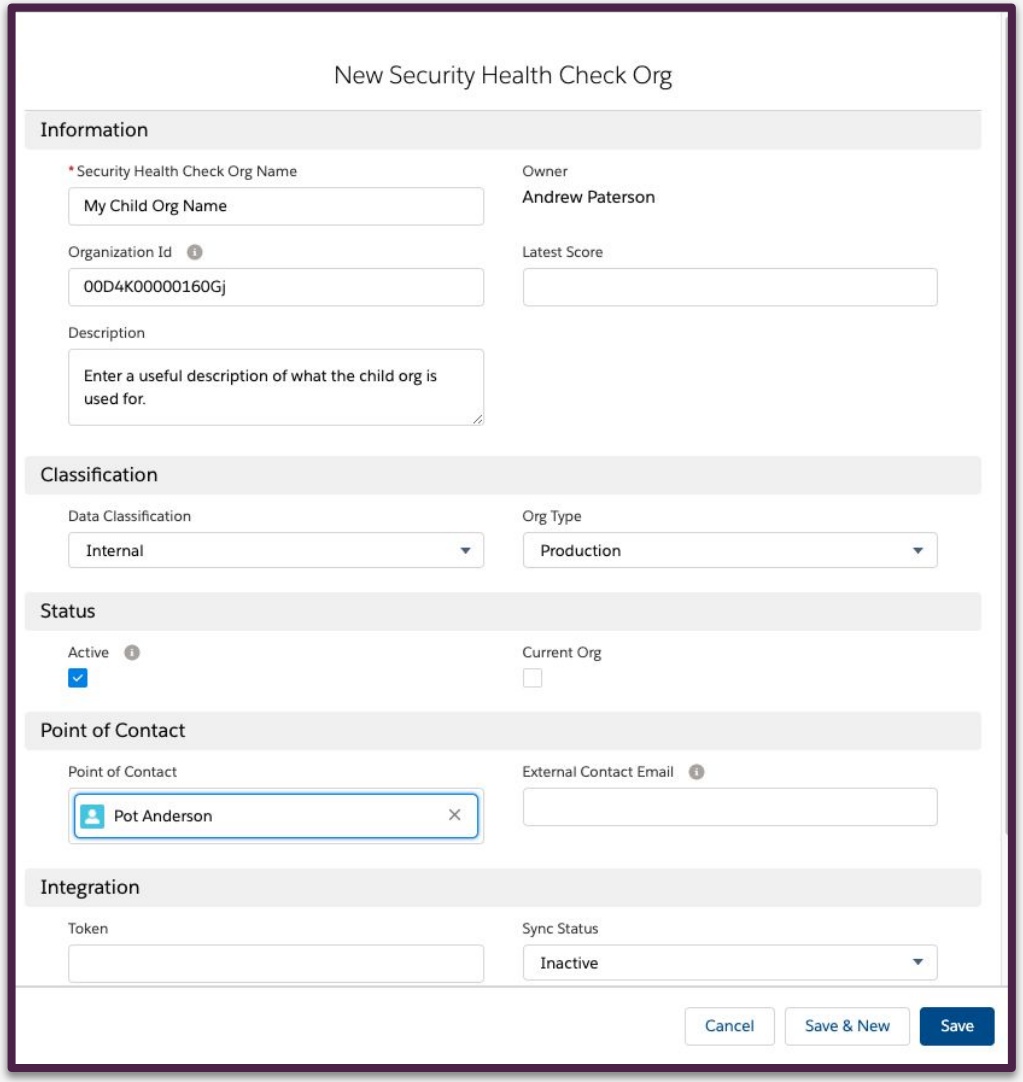
Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to **false.**

Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org

[continued on next page]

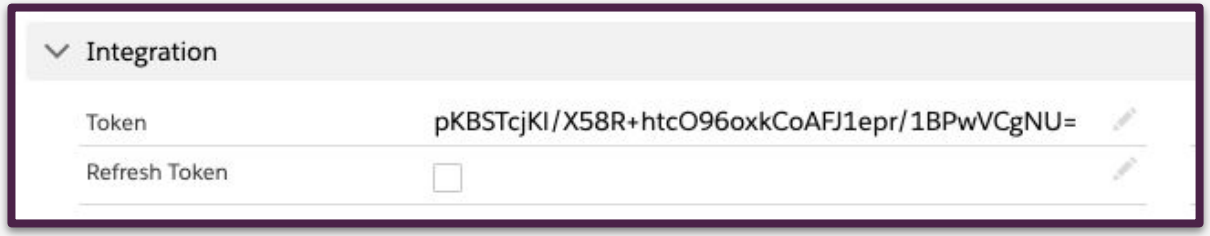


Create Central Security Health Check Record (3/3)

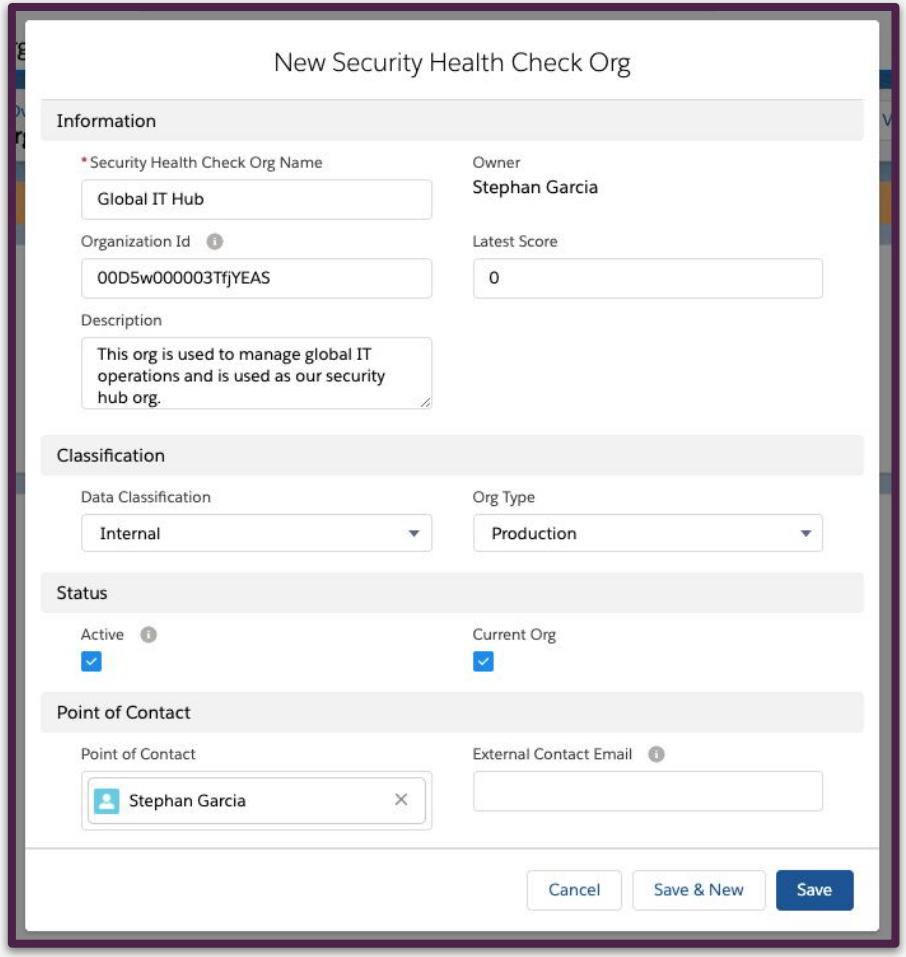
3

Refresh Token : This is used when receiving data via the endpoint, to ensure that the data is from this child org.

Check this option on to ensure that the token is generated on save. (If you need to re-generate the token then edit the record and check the option on again).



Take note of the token that is generated as you will need this in **step 14** when configuring the custom metadata type.



Set Up And Configure The Child Org (1/4)

Start by **installing** the package in the **child** org. We will then work through and configure this org to send data to the central org on a daily basis.

4 Open the *Multi-Org Security* app via the app launcher

5 Open the *Security Health Check Orgs* tab and click *New* to create the org record for this child org. This is needed so that details about the org can appear in the summary page. [See the next page for details of what to provide]

Set Up And Configure The Child Org (2/4)

Security Health Check Org

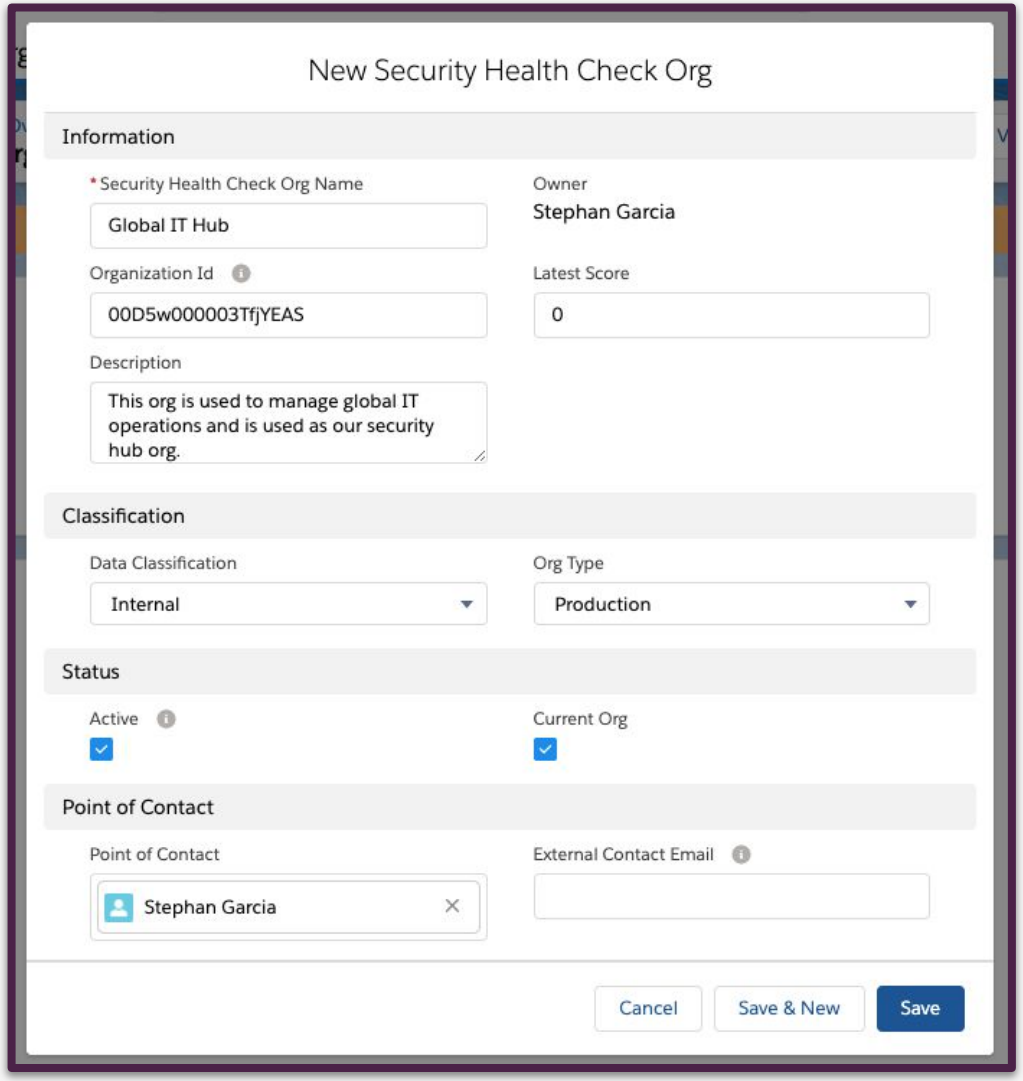
The security health check org record is used categorize and store security health checks against the relevant org.

Name: The name of the Org

Organization Id: The Id of the Org. This can easily be found in the *Company Information* section in *Setup*.

Description: Provide an overview of the purpose of the org

Data Classification: The level of security applied to the org



Set Up And Configure The Child Org (3/4)

Security Health Check Org cont.

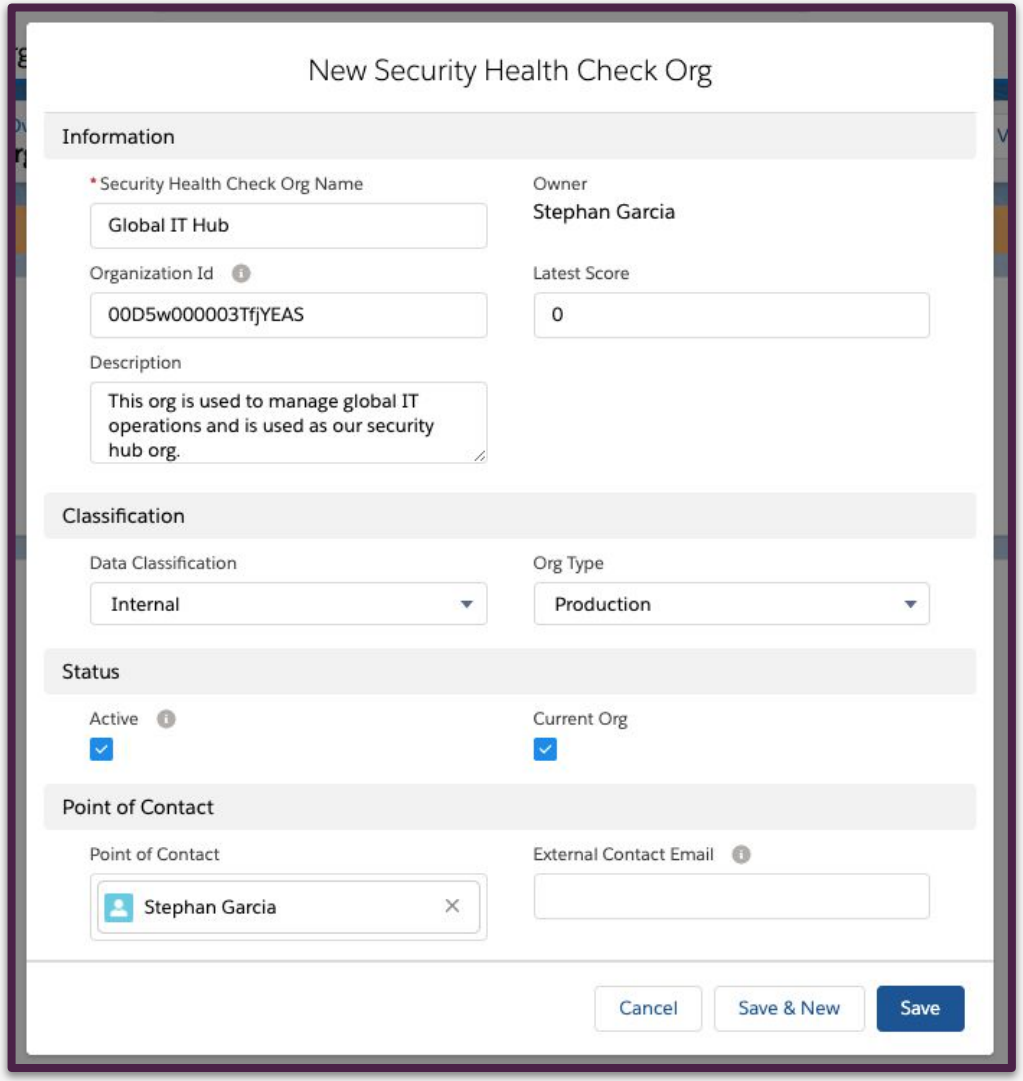
Org Type: Production or Sandbox

Active: True if the org is currently being reported on. Use this toggle to add/remove the org from the summary screens.

Current Org: Set this to true

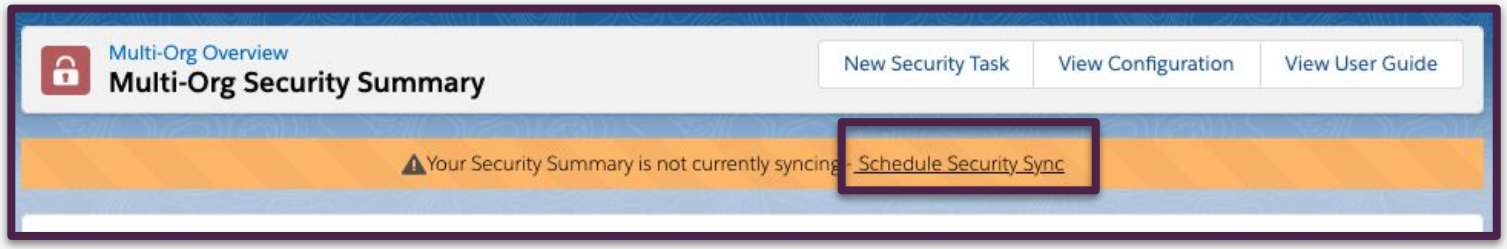
Point of Contact: The main point of contact for the org

External Contact Email: The email of the point of contact if they are not a user in this Salesforce org



Set Up And Configure The Child Org (4/4)

6 Navigate to the summary page and you should see the following information.



We will return later to set up and run the sync job. Before that we need to configure the reporting end point and appropriate security method.

If you are using the *Connected App* method for sending data to the central org, then proceed with Step 7.

If you are using the *Salesforce site public service* method, you can jump ahead to step 13.

Option 1 - Connected App Method

Child Org - Connected App Method (1/5)

7 Create an Auth Provider

Navigate to Setup > Auth. Providers

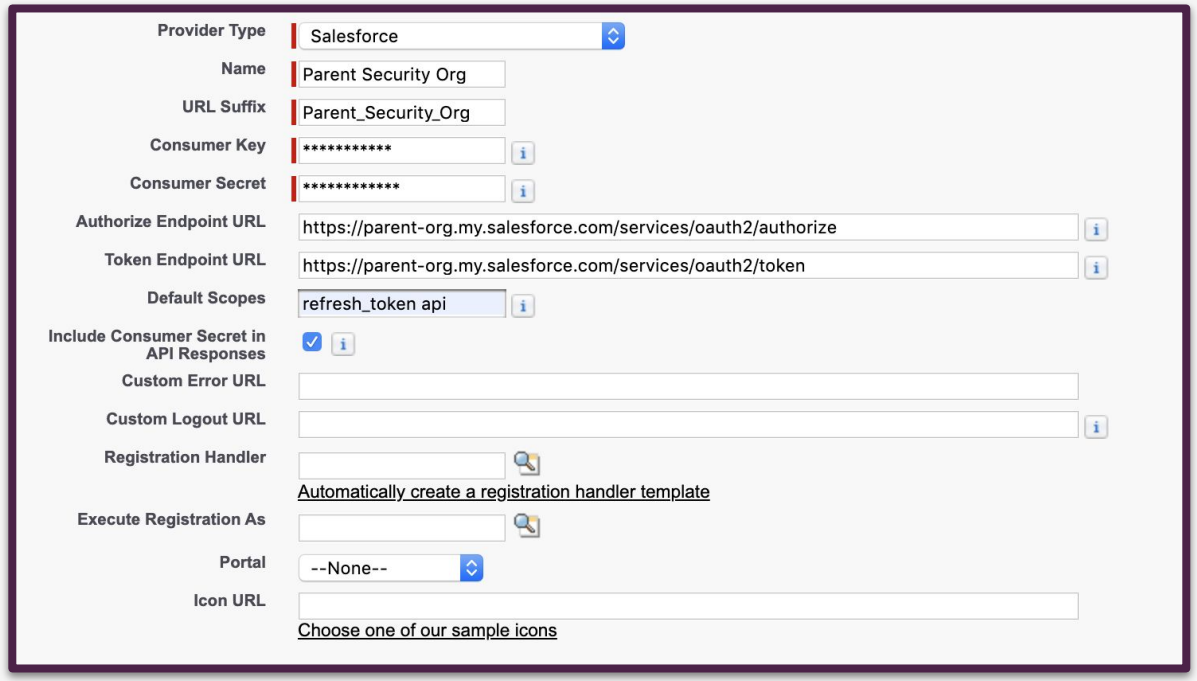
Create a new Auth Provider

Provider Type: Salesforce

Name: Designate it a memorable name

Consumer Key & Consumer Secret:
From the central org connected app we created

Child Org



Central Org

Child Org - Connected App Method (2/5)

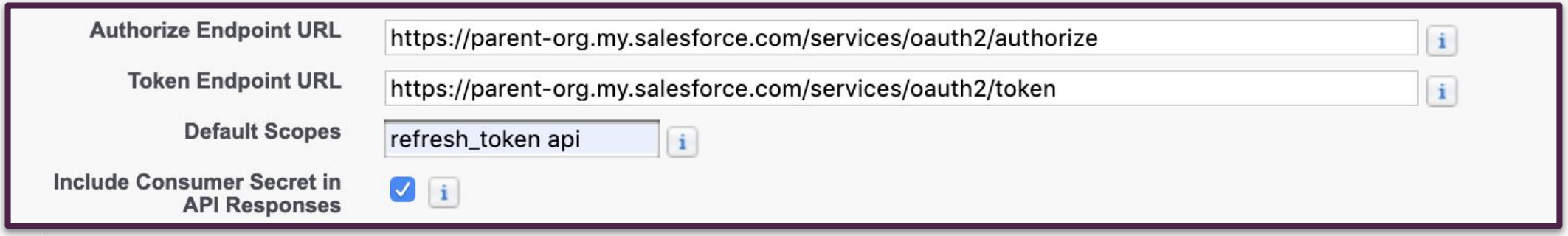
8 Create an Auth Provider (cont.)

Authorize Endpoint: https://**central-org-domain**.my.salesforce.com/services/oauth2/authorize

Token Endpoint: https://**central-org-domain**.my.salesforce.com/services/oauth2/token

Default Scopes: refresh_token api

Include Consumer Secret In Api Responses: True



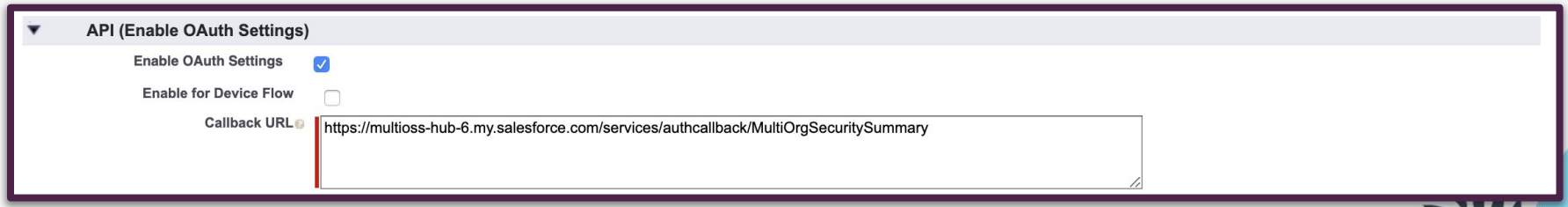
Child Org - Connected App Method (3/5)

9 Save the auth. provider

When saved, copy the callback URL. We need to copy this into the **central** connected app configuration.

10 Update the connected app record

Open the central connected app configuration and populate the Callback URL. If this is the first child org you will need to replace the Temporary Callback URL we set earlier. **Note:** You can have one callback url per line.



Child Org - Connected App Method (4/5)

11 Set up the Named Credentials

The child org scheduled service uses Named Credentials when making the call out to the central org.

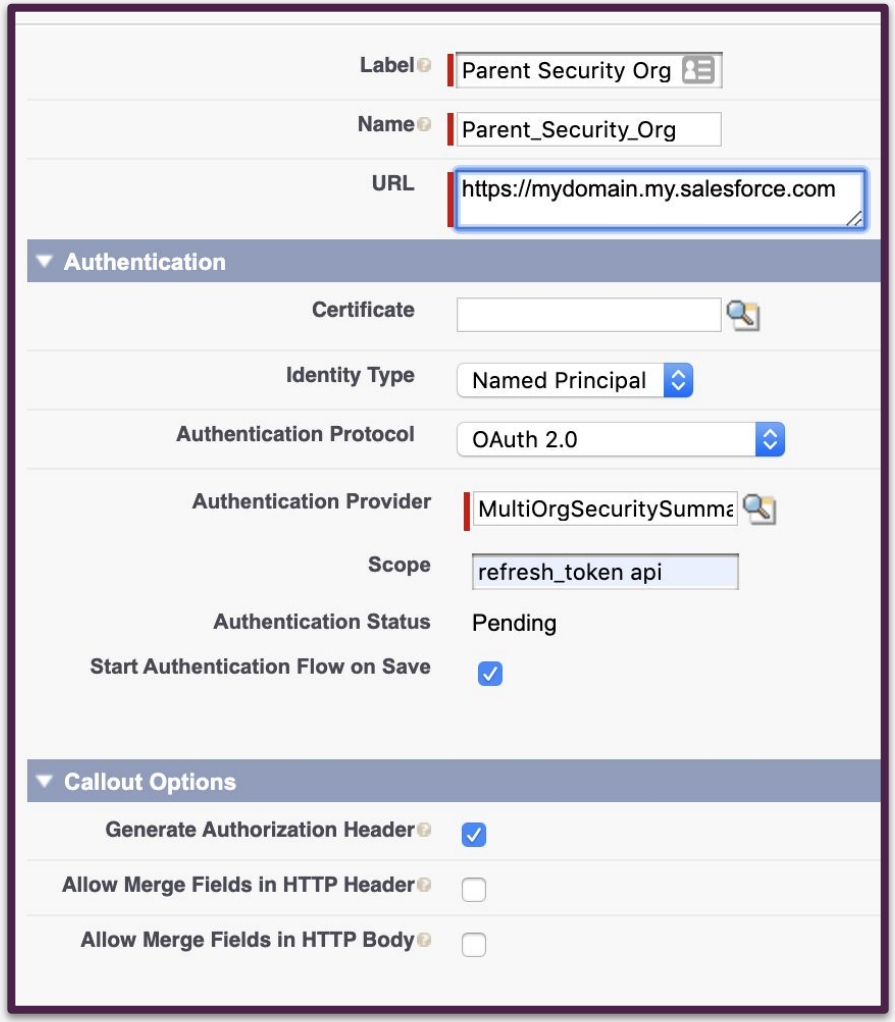
Back in the child org, navigate to *Setup > Named Credentials*

Name: Designate it a memorable name

URL: https://**mydomain**.my.salesforce.com (This is the central domain URL and needs to be the ...my.salesforce.com URL for Authenticated users or the force.com URL for the sites method)

Identity Type: Named Principal

Authentication Provider: The Auth Provider we just created



Child Org - Connected App Method (5/5)

Set up the Named Credentials (cont.)

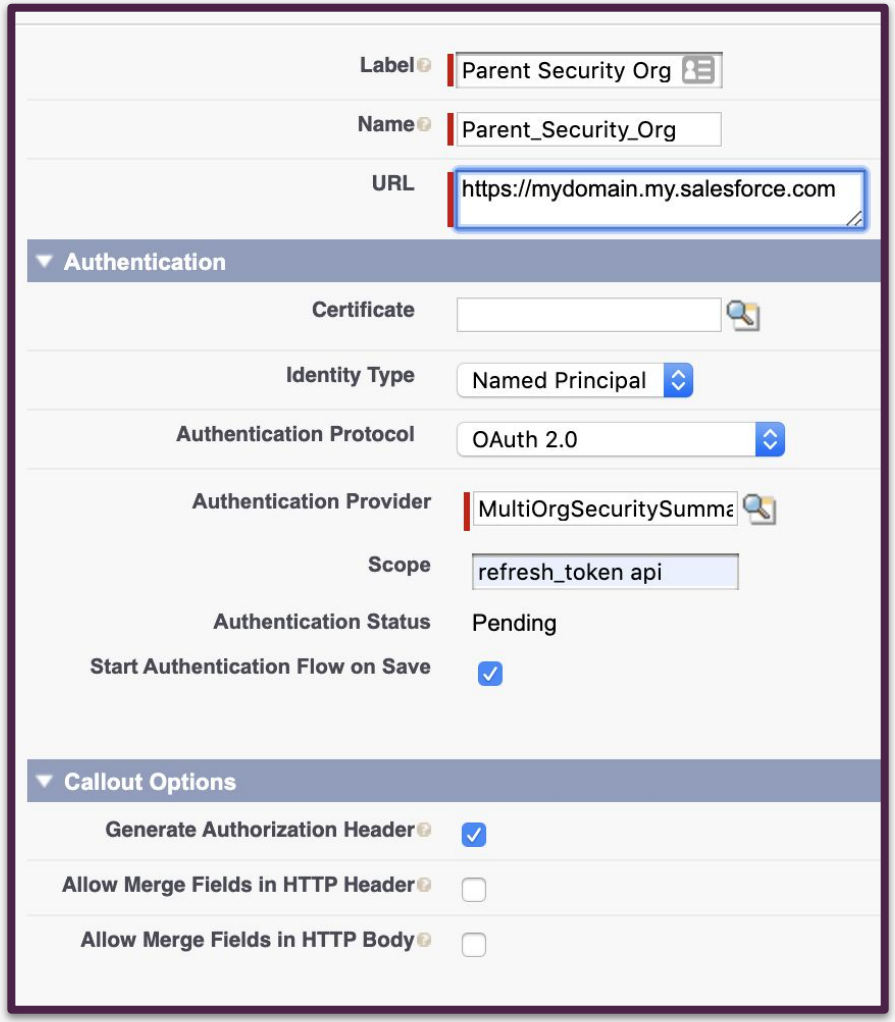
Scope: refresh_token api

Start Authentication Flow on Save: True - this will allows to authenticate the central org with our credentials

Generate Authorization Header: True

12 Save the named credential

On saving the record you will then ask you to log into the central org. Login, and you're now authorized.



Option 2 - Saleforce Sites Method

Child Org - Salesforce Sites Method

13 Set up the Named Credentials

Navigate to *Setup > Named Credentials*

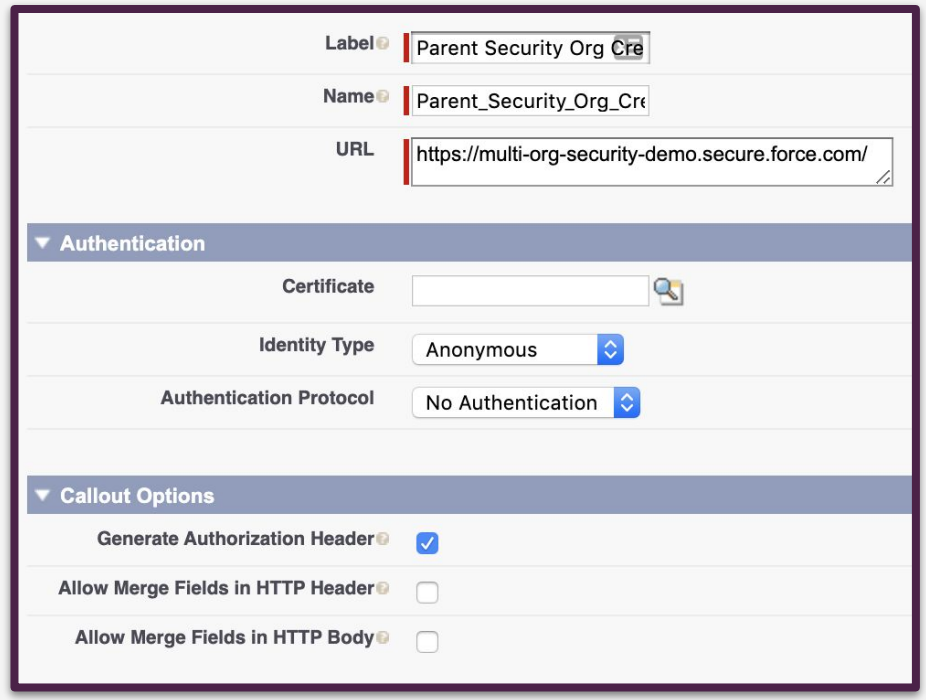
Label: Designate it a memorable name

URL: The secure url of the central site you created earlier

Identity Type: Anonymous

Authentication Protocol: No Authentication

Generate Authorization Header: true



You will need the Developer Name (Name field) for the next steps.

Finalise the Child Org Configuration

The following instructions apply regardless of whether you are using Option 1 or Option 2.

Child Org - Metadata configuration (1/2)

14 Clone the Security Health Check Config

Navigate to *Setup > Custom Metadata Types*

Select *Manage Records* for the Security Health Check Config record and then select *Configuration* in the configs list.

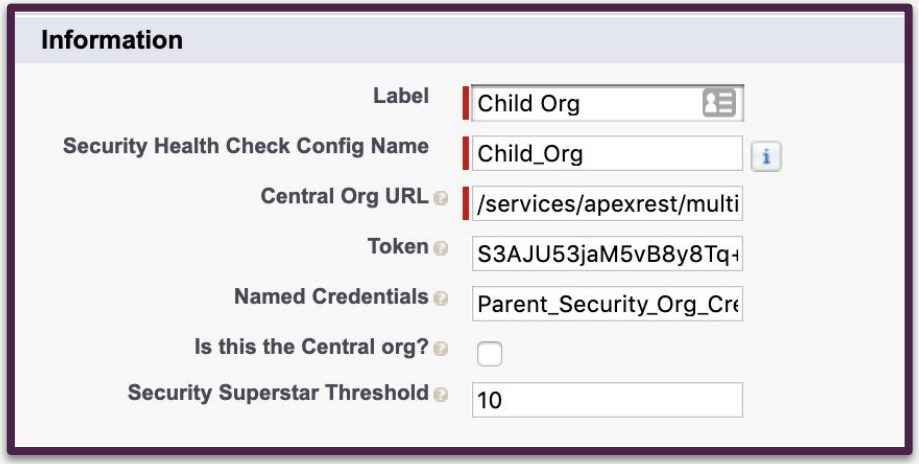
Clone the record.

Label: Give this a label that allows you to identify the record

Security Health Check Config Name: Make sure you change this to reflect the Label above. *[If the Name is left as Configuration, it will be ignored and the sync will not work !]*

Central Org URL: Leave as the default

[continue on the next page]



Child Org - Metadata configuration (2/2)

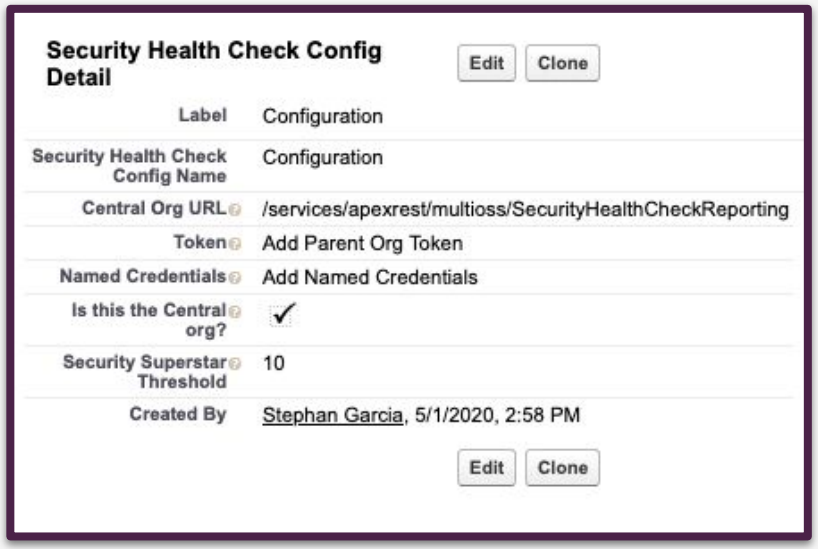
Token: Enter the token belonging to the **child** org that was created earlier in the **central** org.

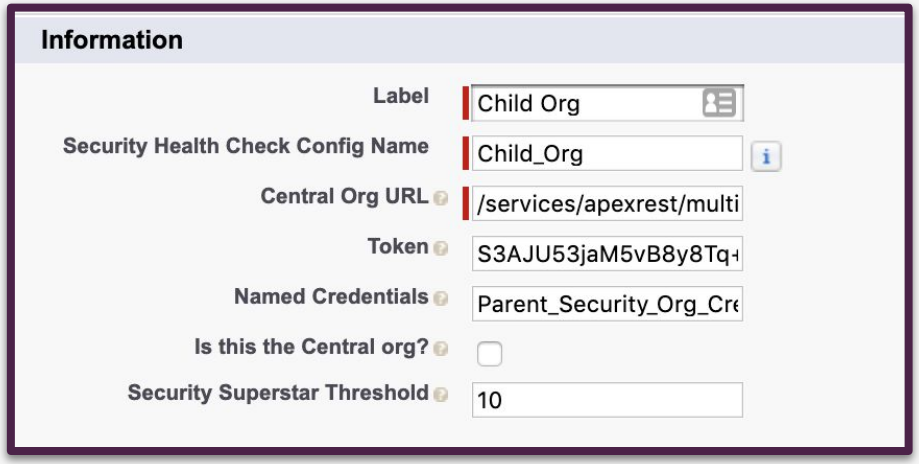
This token will be sent with the reporting data and needs to match the central org record to be saved.

Named Credentials: The name of the named credential you've just created.

Is this the central org: False. This setting controls whether you see the multi-org version of the app page, or the single org version.

15 **Save** the record



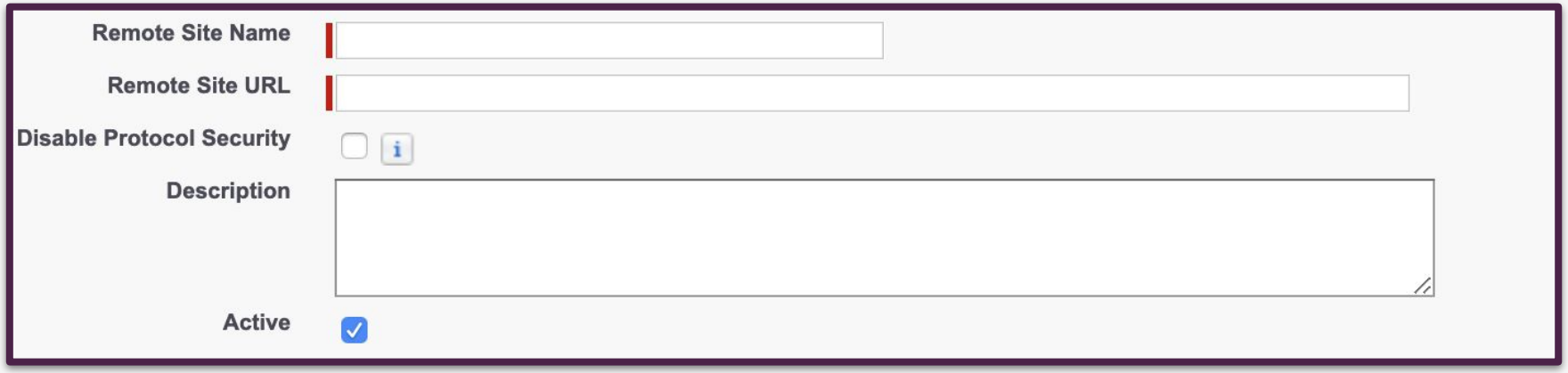


Create Remote Site Settings

Create Two Remote Site Settings in the Child Org

Navigate to *Setup* > *Remote Site Settings*

16 **Create Remote site Setting 1:** https://**central-org-mydomain**.my.salesforce.com
The mydomain url for the central org will allow us to send the health checks



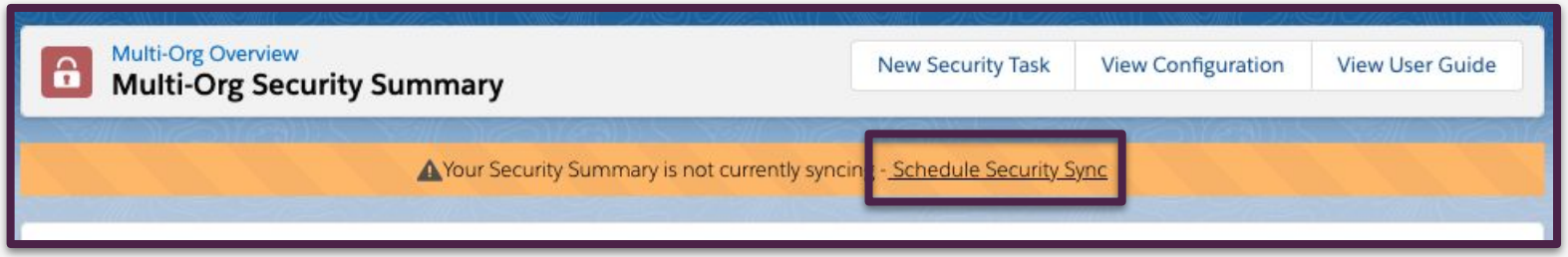
17 **Create Remote Site Setting 2:** https://**this-org-mydomain**--c.visualforce.com
This link for the child org will allow us to get the Health Check from the Tooling API

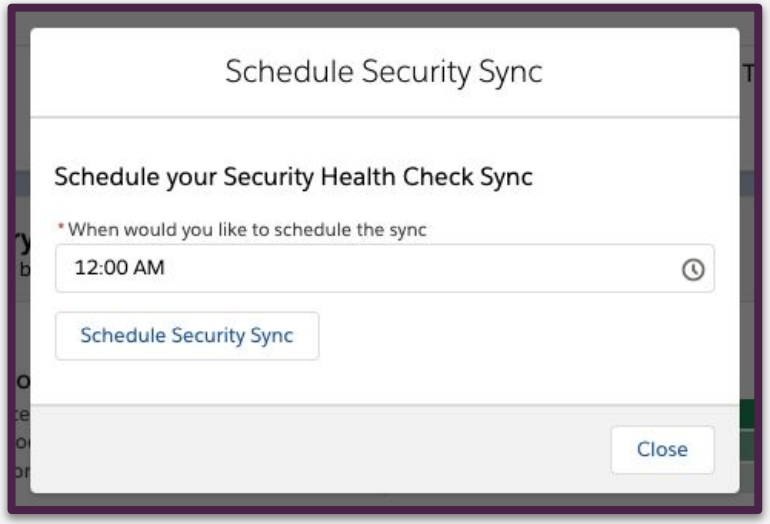
Schedule the Health Check Sync

18

Navigate to the Multi-Org Security Summary tab in the child org and select '*Schedule Security Sync*' from the warning banner that is displayed.

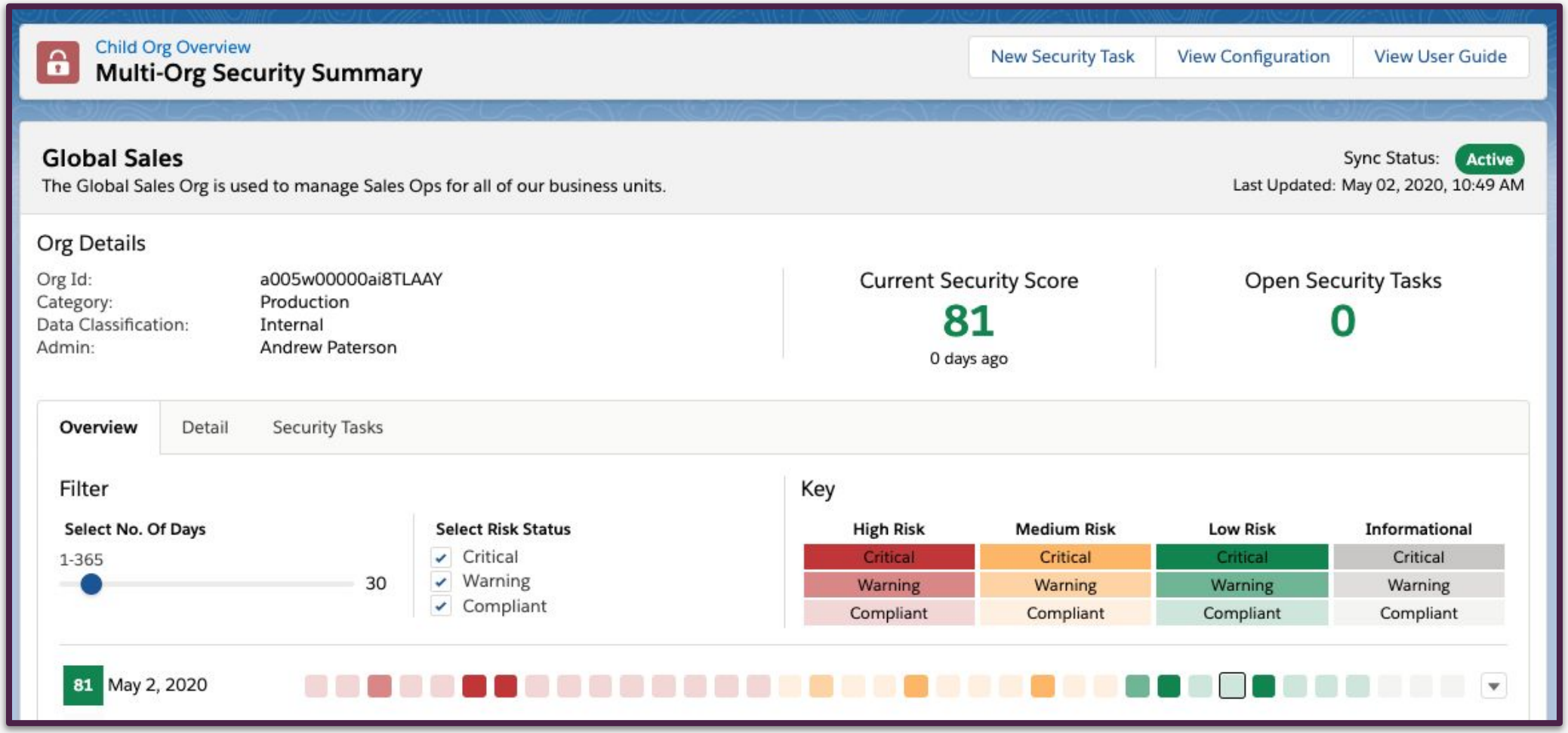
This will allow us to sync the first health check and write the data to this org. Once completed, schedule the daily sync from the next prompt. This can be changed at any time.





Schedule your Health Check Sync

Once the job has run, you will see that the job has been completed in your child org and it is now active

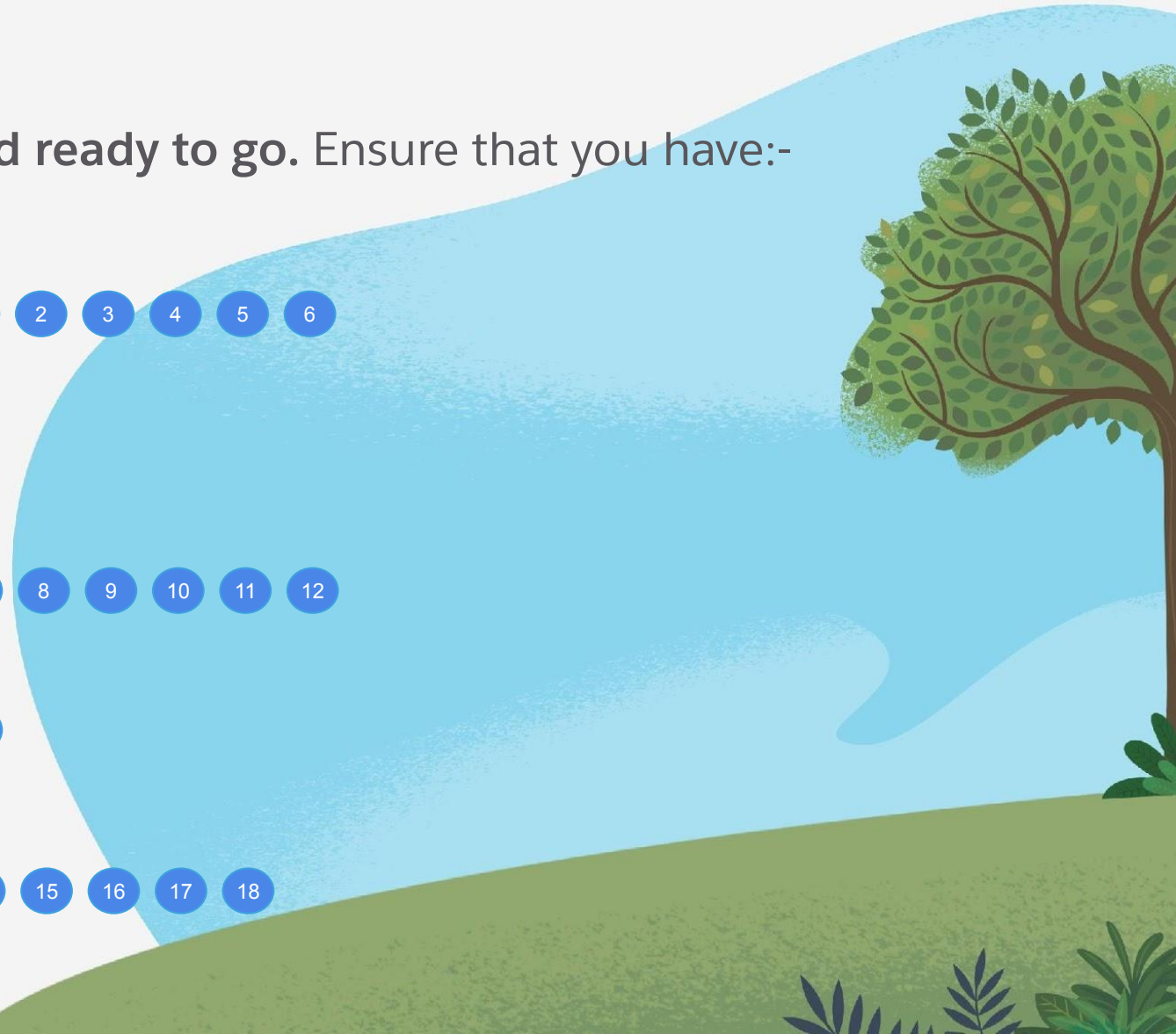


Child Org Checklist

That should be the child org configured and ready to go. Ensure that you have:-

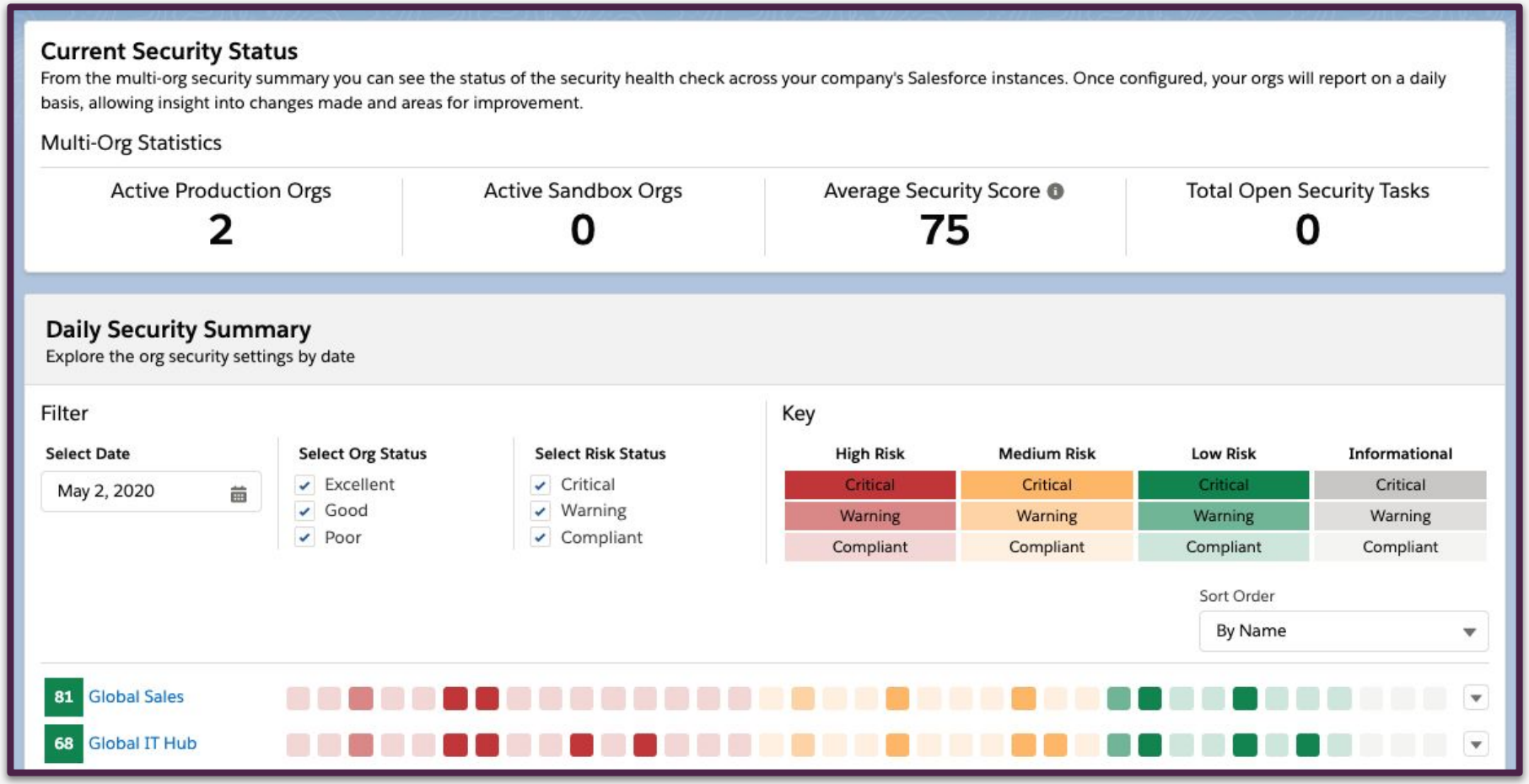
- Set Up The Child Configuration 1 2 3 4 5 6
- Set up the Reporting Method
  - Connected App Method 7 8 9 10 11 12

    OR
  - Public Site Method 13
- Finalised the Child Org Configuration 14 15 16 17 18

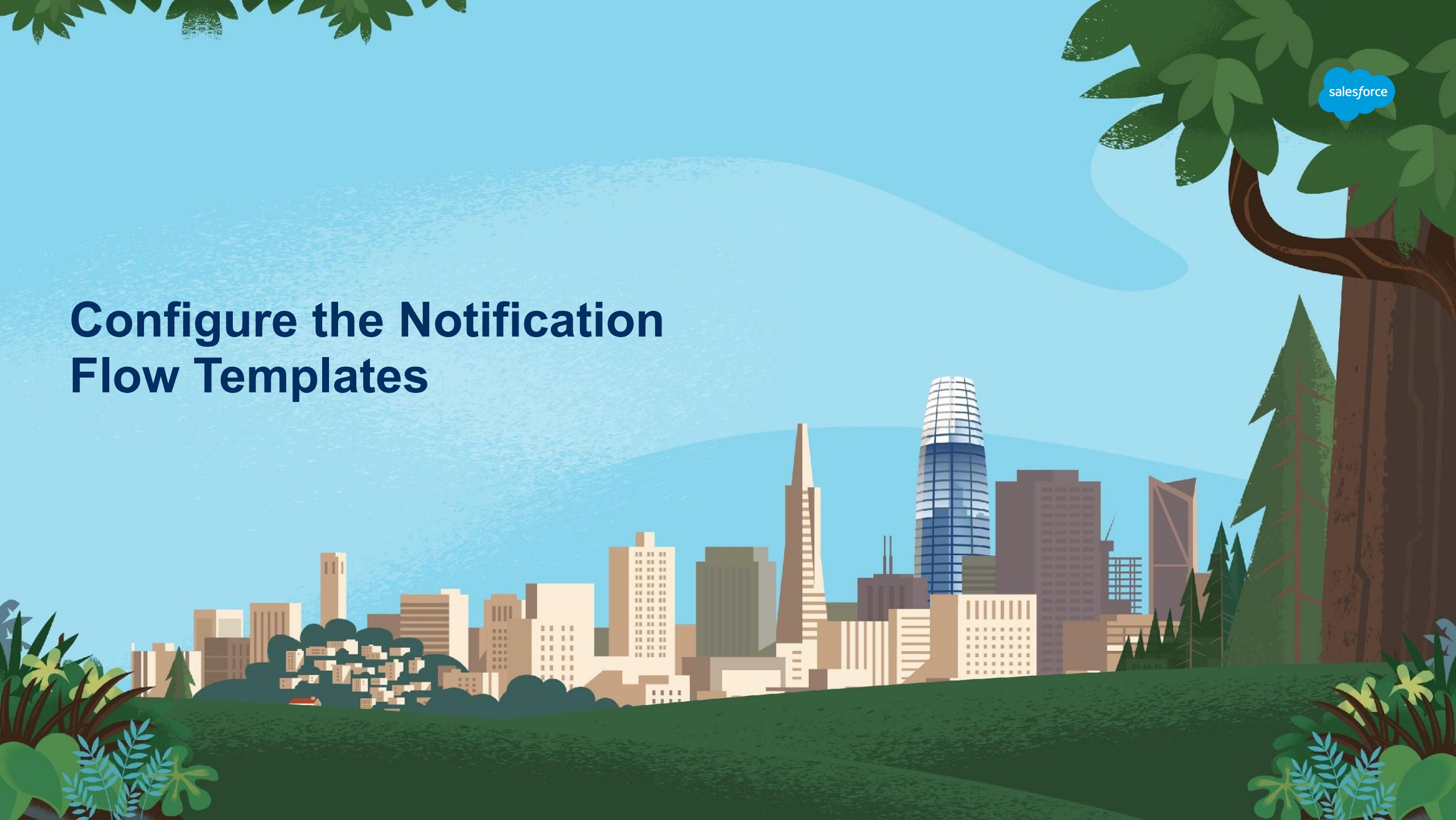


Verifying the Result

You can see in your Central org that we now have a health check record for the child org. Repeat the steps for any child or you would like to add to Multi-Org Security Summary!



Configure the Notification Flow Templates



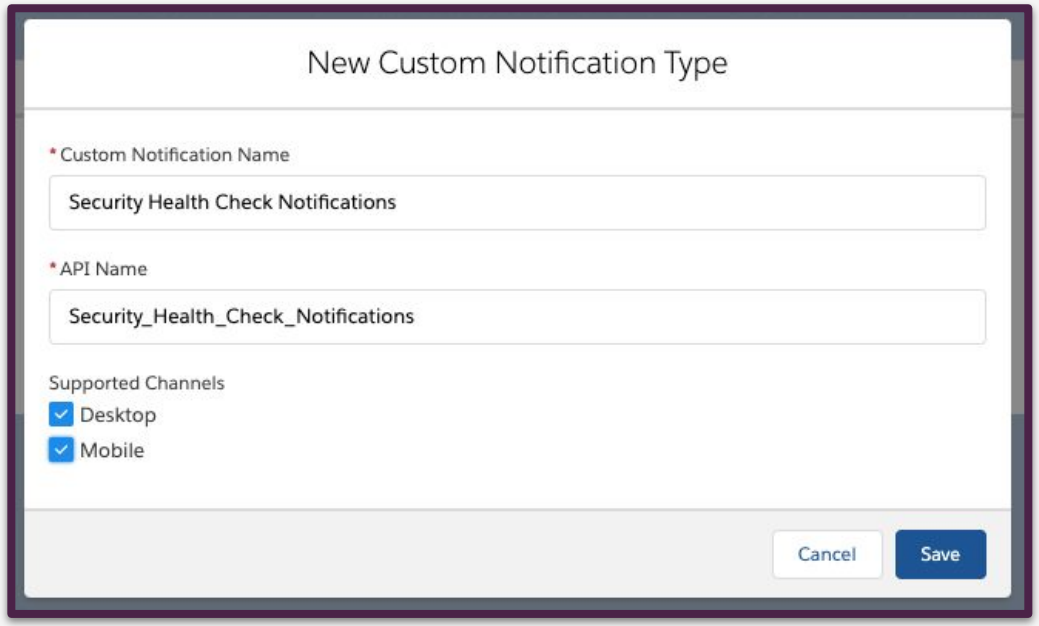
Create A Custom Notification Type

A custom notification type will be used to alert your admins when the status of their security health check has changed.

Navigate to Setup > Custom Notification types

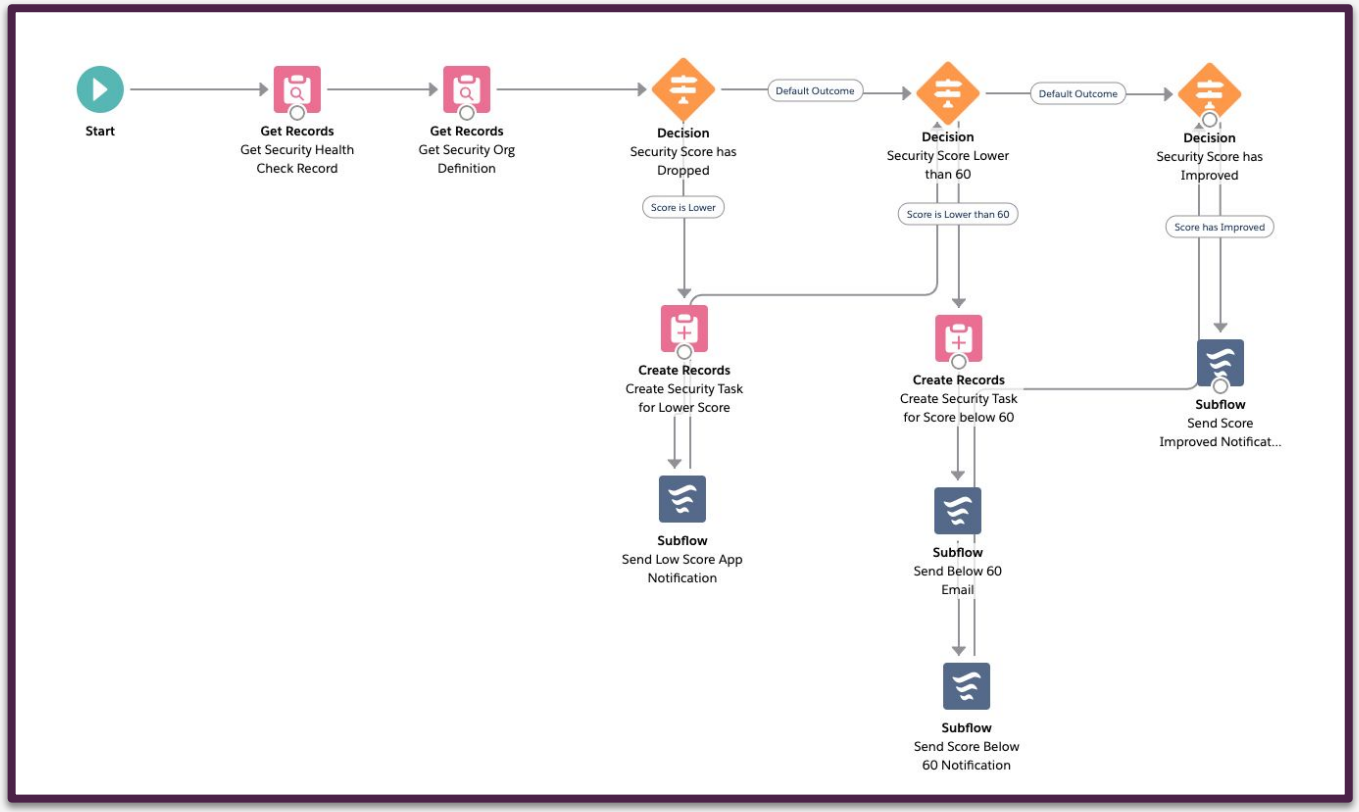
Notification Name: Security Health Check Notifications

Supported Channels: You can send notifications on the desktop and to users Salesforce mobile app



Security Summary Evaluation Flow Template

Using flow, you have the ability to evaluate the Security Health Check when it has been created and check for any anomalies.

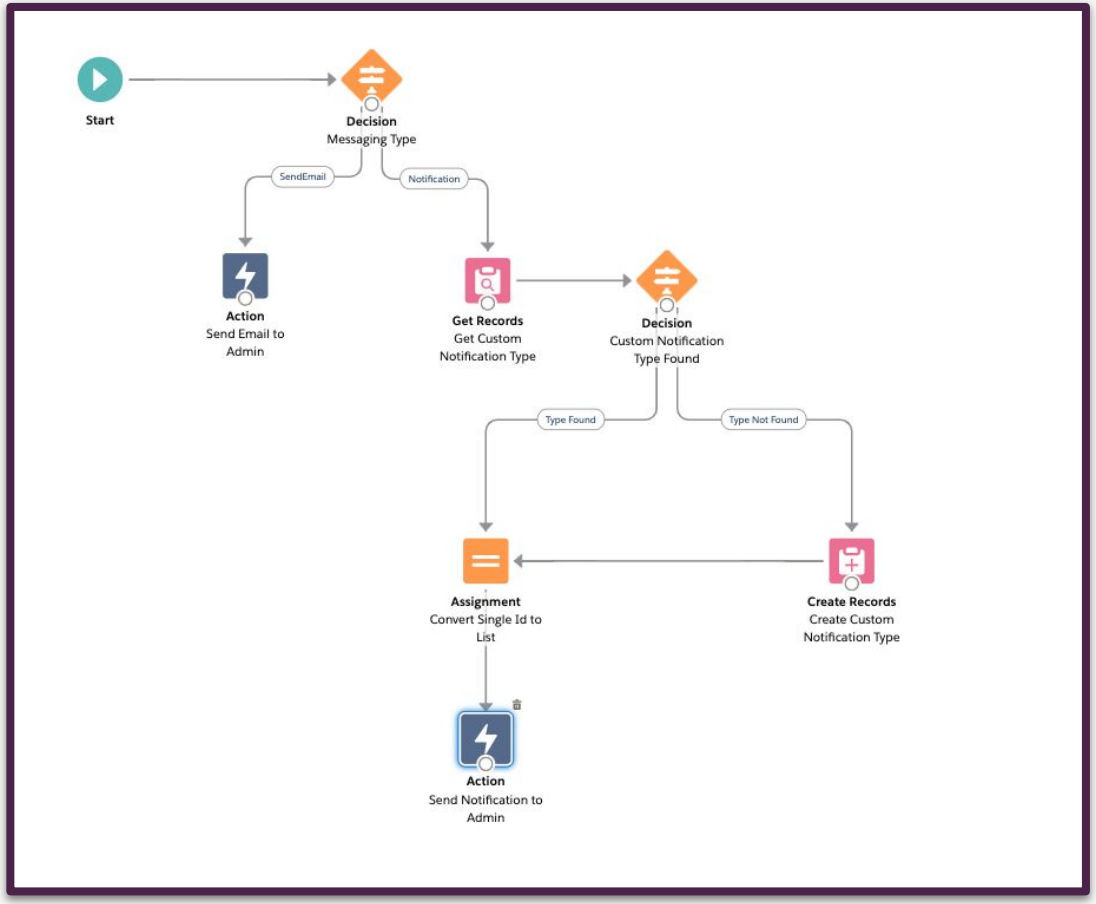


Security Summary Notification Flow Template

Using flow, you have the ability to send email and in-app notifications to Admin users who have had a security report generated.

You must supply the type of notification, email or notification. Then supply either the Admins email address or record Id.

This will then let them know that they have a security action that needs to be taken care of.



Security Tasks

Security Health Check Tasks

Security Tasks are used to assign actions to your team of admins who are responsible for managing the security of your salesforce orgs!

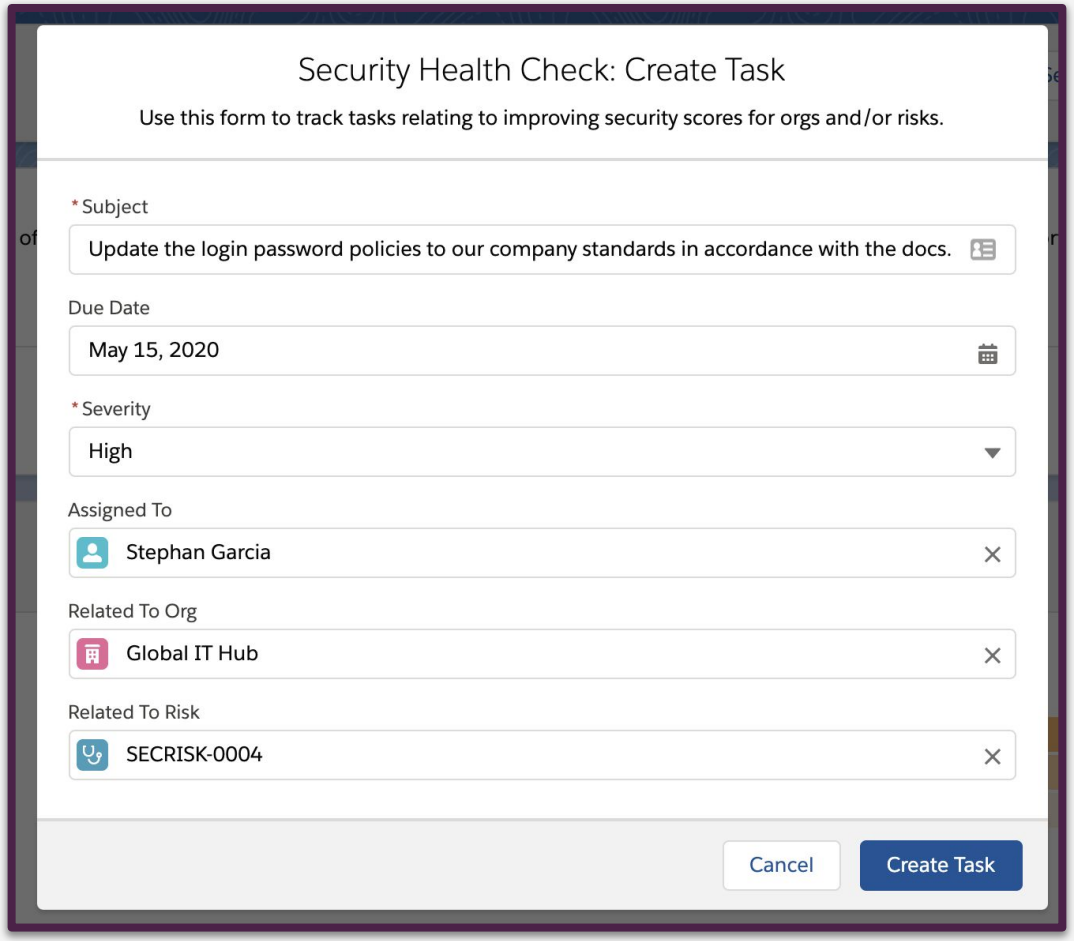
Subject - the instructions that you would like your user to action.

Assigned to: Designate an Admin to complete this task

Related to Org: Select which org this security task is related to

Related to Risk: The risk that this task is associated to.

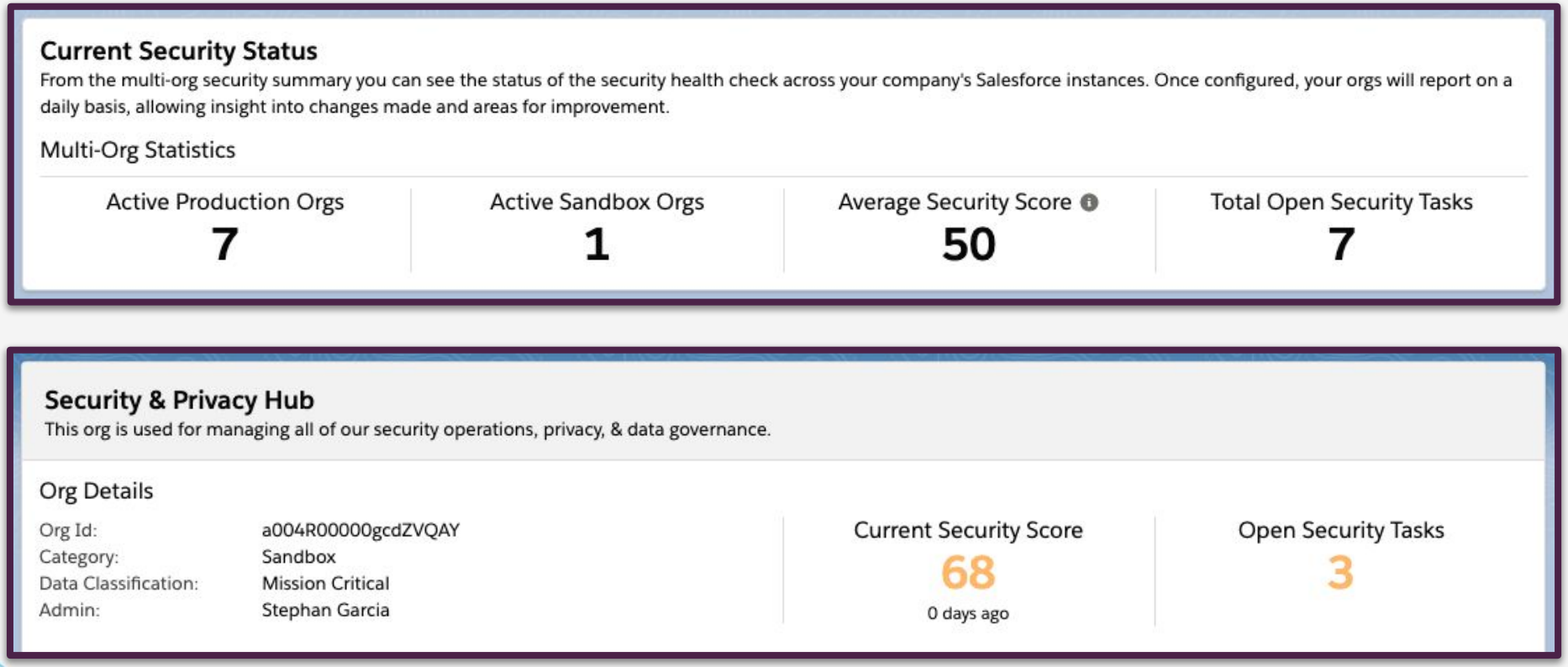
A task does **NOT** need to be associated to a specific org, risk or user



Security Health Check Tasks

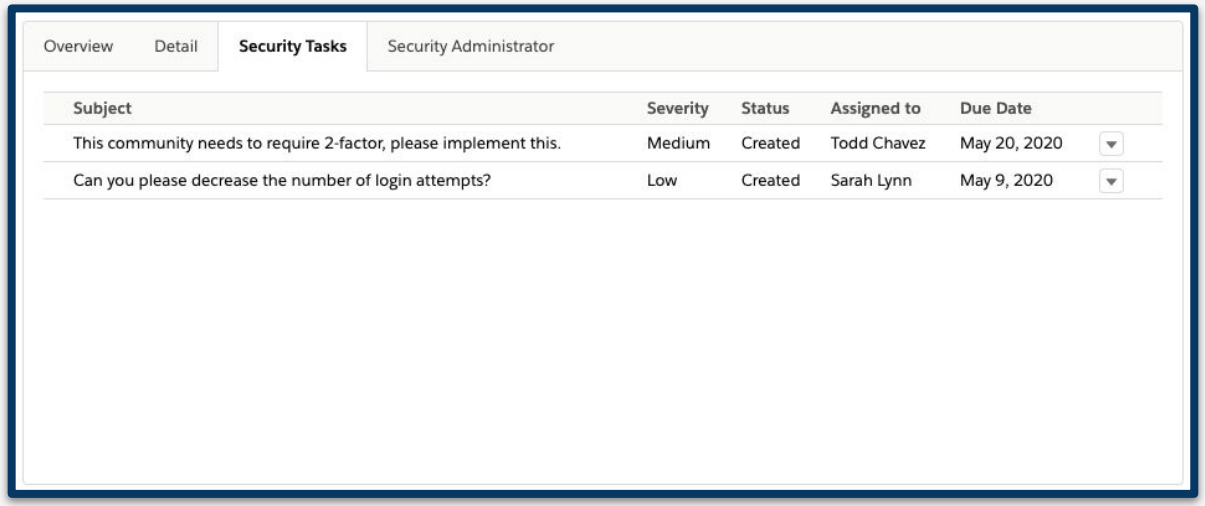
Open Task Notifications

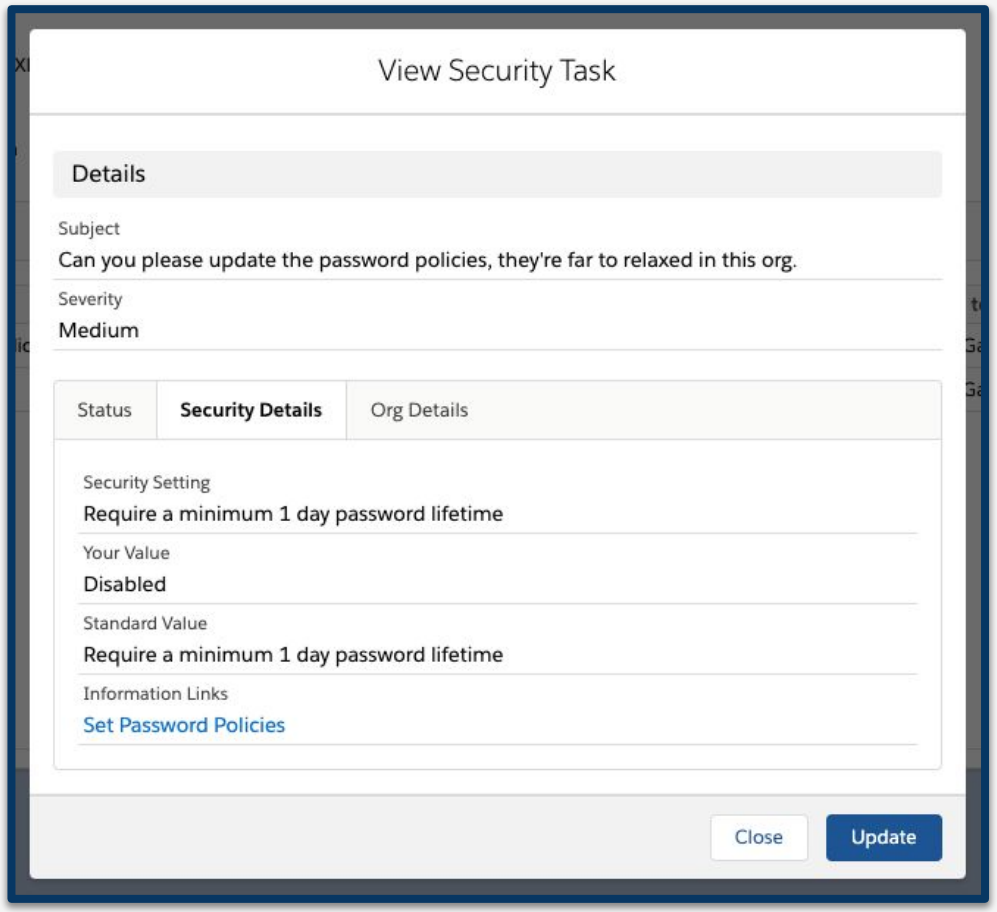
When you are viewing the multi-org overview or a single org, you can see the number of relevant open tasks.



Security Health Check Tasks

If the Security Task is linked to a risk - the Admin will have direct access to any relevant documentation that will help them fix the vulnerability.

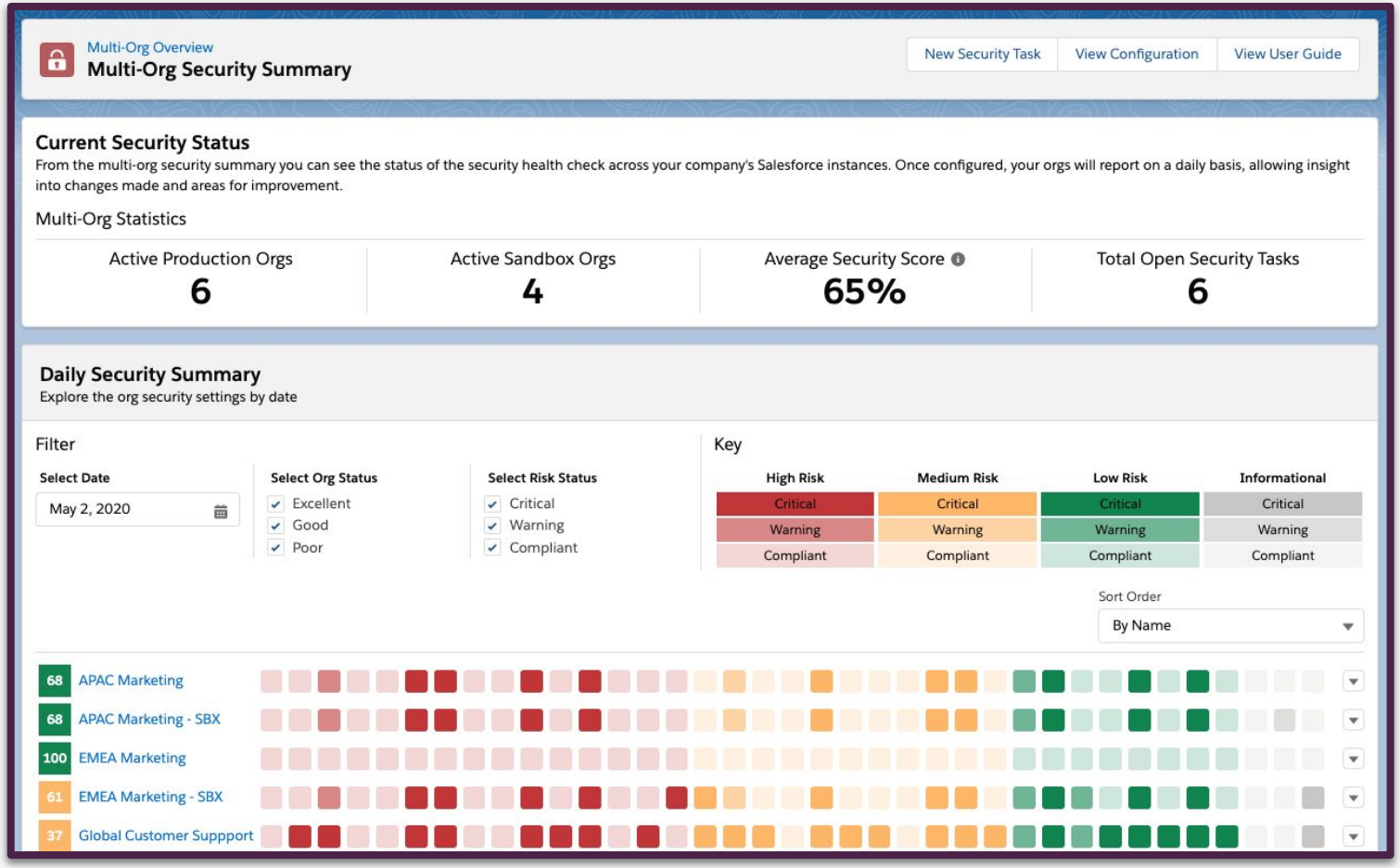




Navigating Multi-Org Security Summary

Navigating Multi-Org Security Summary

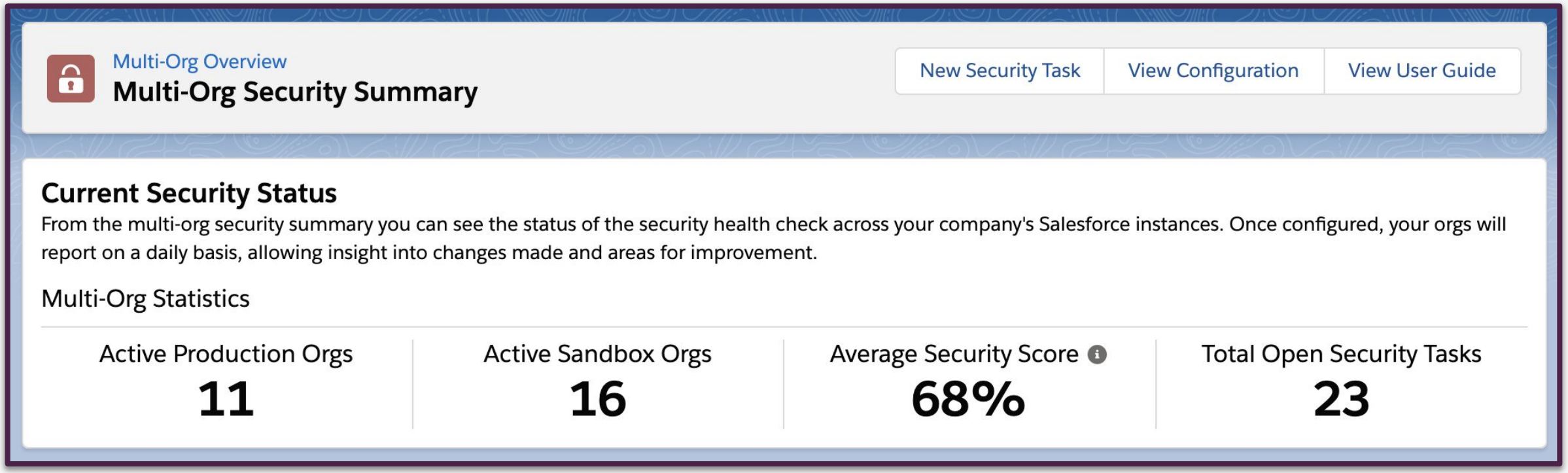
Now that we have the app setup - lets take a look at it's features.



Navigating Multi-Org Security Summary

Central Org - Multi-Org Security Status

When you first navigate to the Multi-Org Security Summary - you can see an overview of all of the associated orgs that are syncing to your central org, along with their stats.



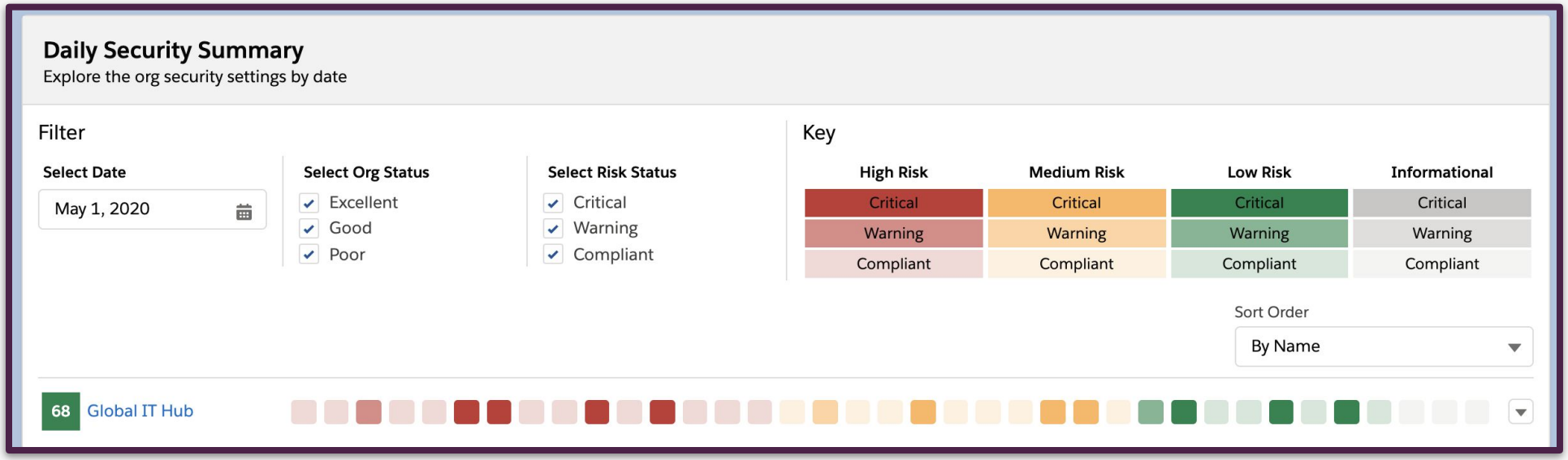
Navigating Multi-Org Security Summary

Central Org - Daily Security Summary

The daily security summary is where you will find an overview of ALL of your configured Salesforce Orgs

Filter: You can filter this view by Date, Org Security Status, and Risk Status

As you can see, the darker the shade of the risk, the more important it is for the risk to be resolved.



Navigating Multi-Org Security Summary

Central Org - Daily Security Summary

When you hover over a risk item, you will be shown a pop-over containing information about the risk.

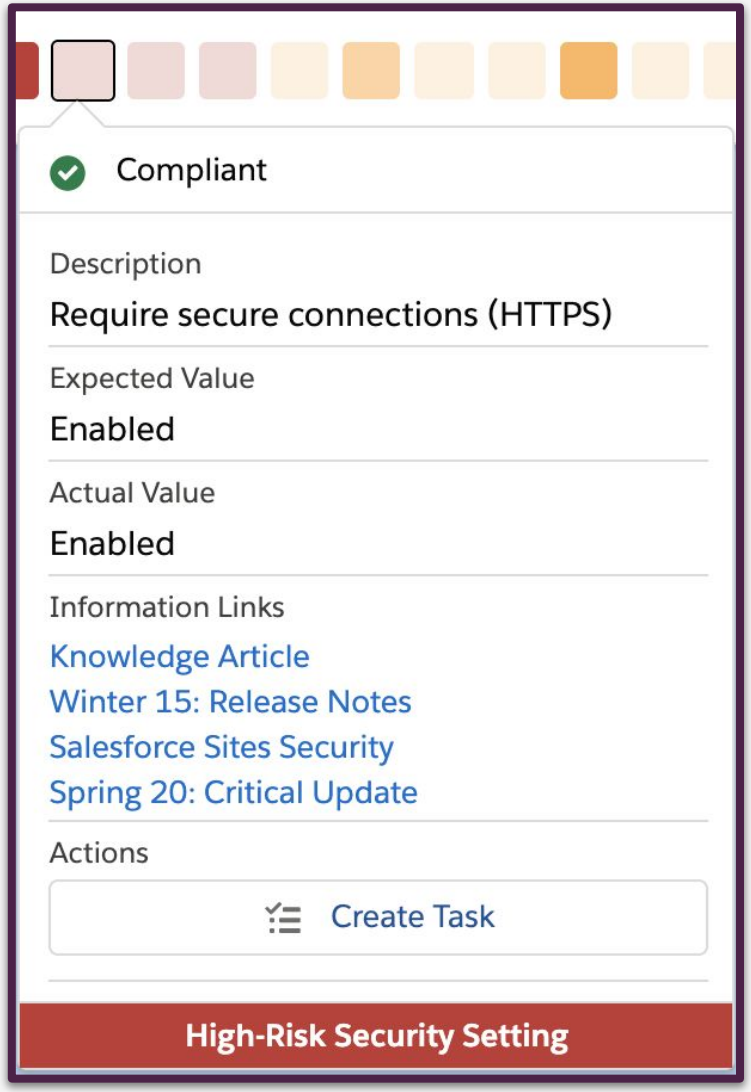
Description: You can see the security risk that has been selected

Expected Value: The value that Salesforce regards as secure

Actual Value: Your current security setting in this org

Description: Links to the relevant documentation needed to solve the security issue

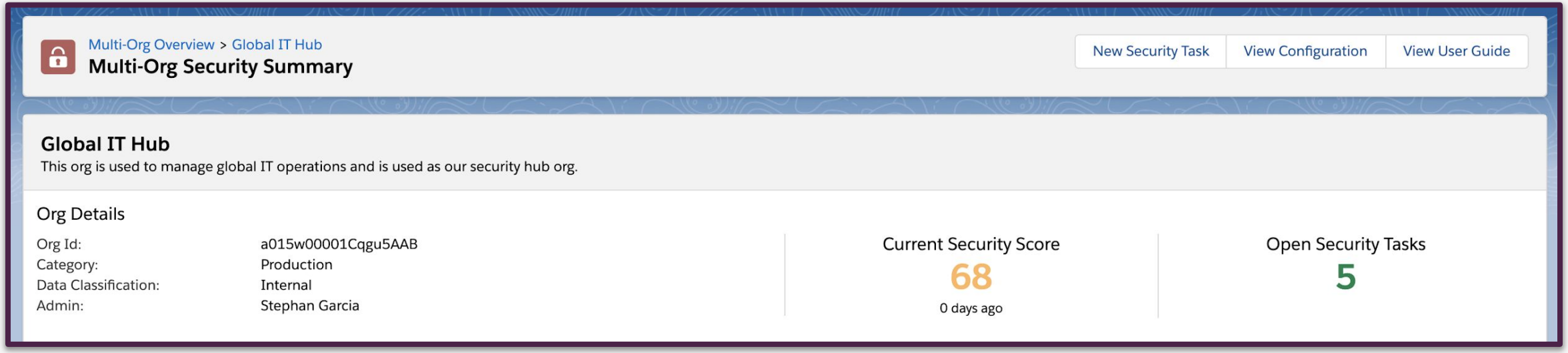
Actions: You can create a task for the admin that is responsible for this org



Navigating Multi-Org Security Summary

Central Org - Selected Org

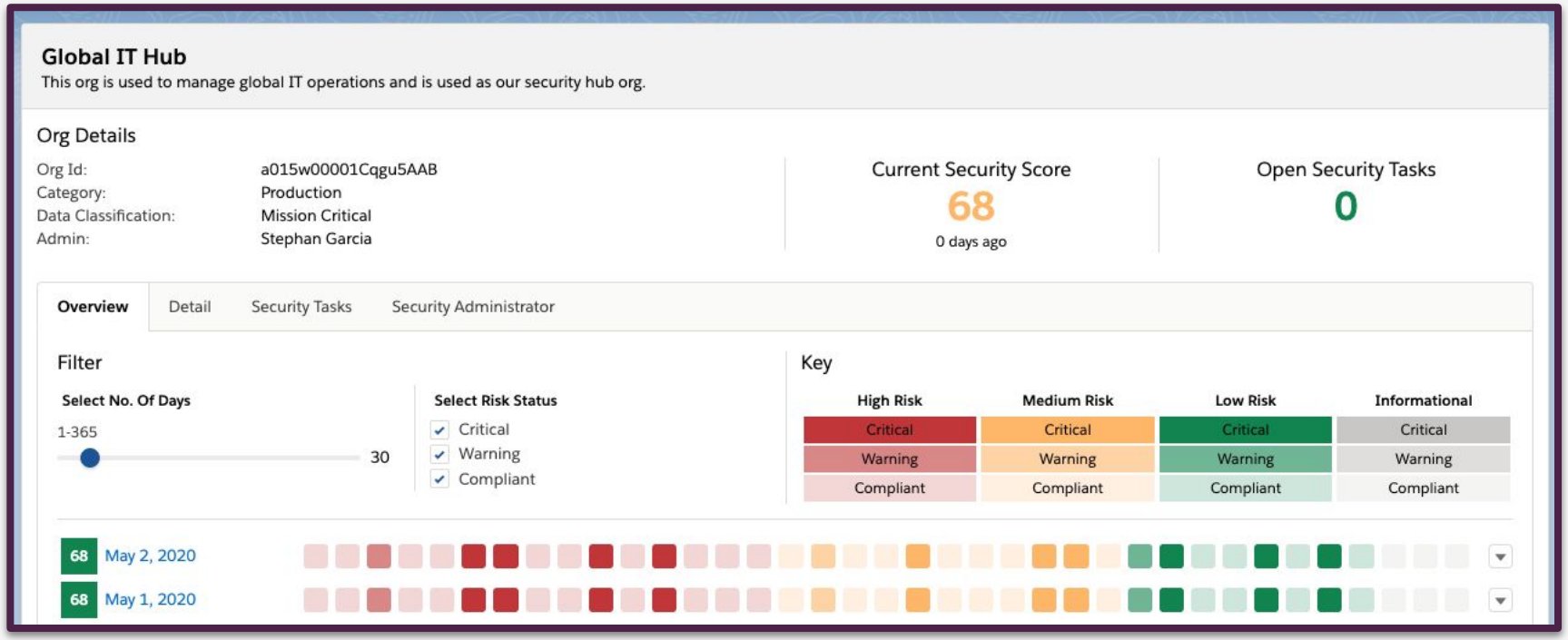
You can select the name of the child org and navigate to a detailed view of that org.



Navigating Multi-Org Security Summary

Central Org - Selected Org

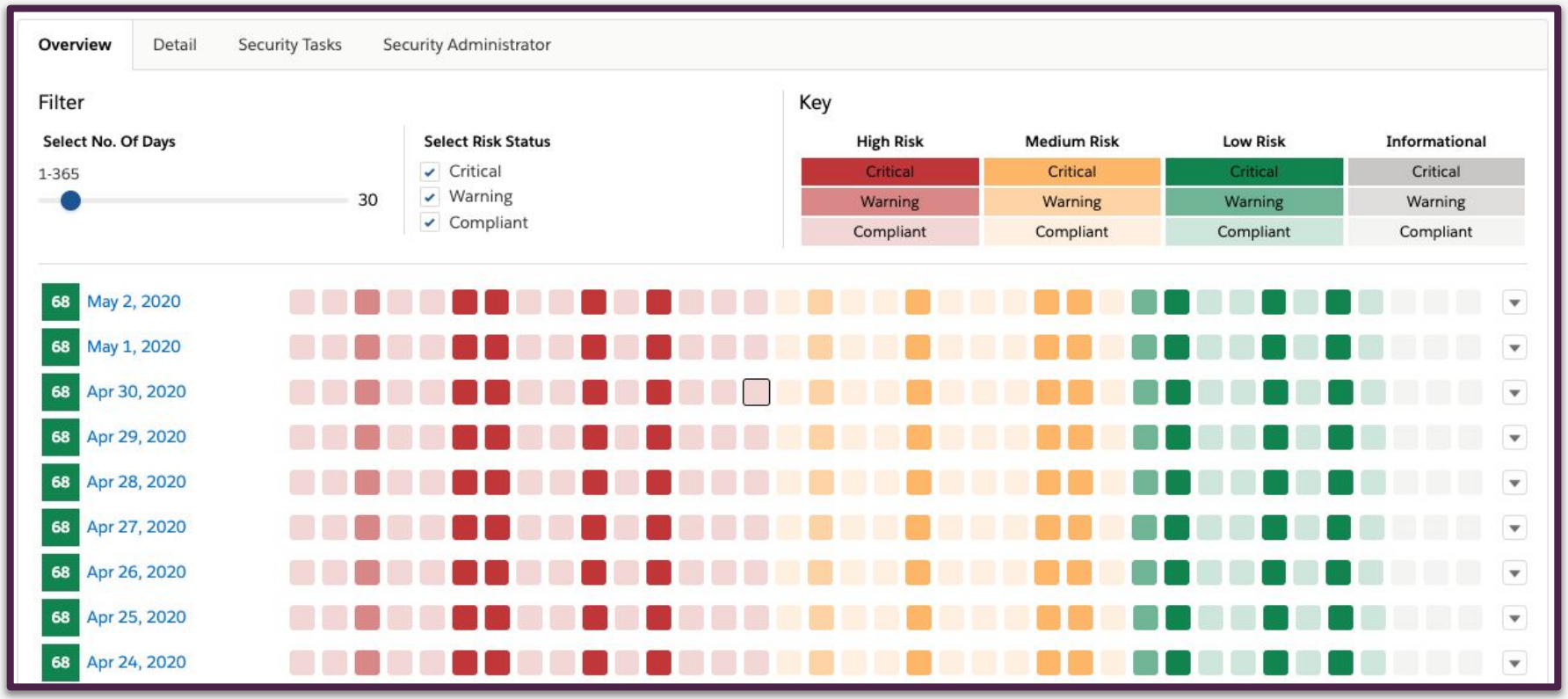
You can select the name of the child org and navigate to a detailed view of that org. The single org view will give you the options to view the daily overview, the detail of health check, the security tasks, and the admin.



Navigating Multi-Org Security Summary

Selected Org - Overview

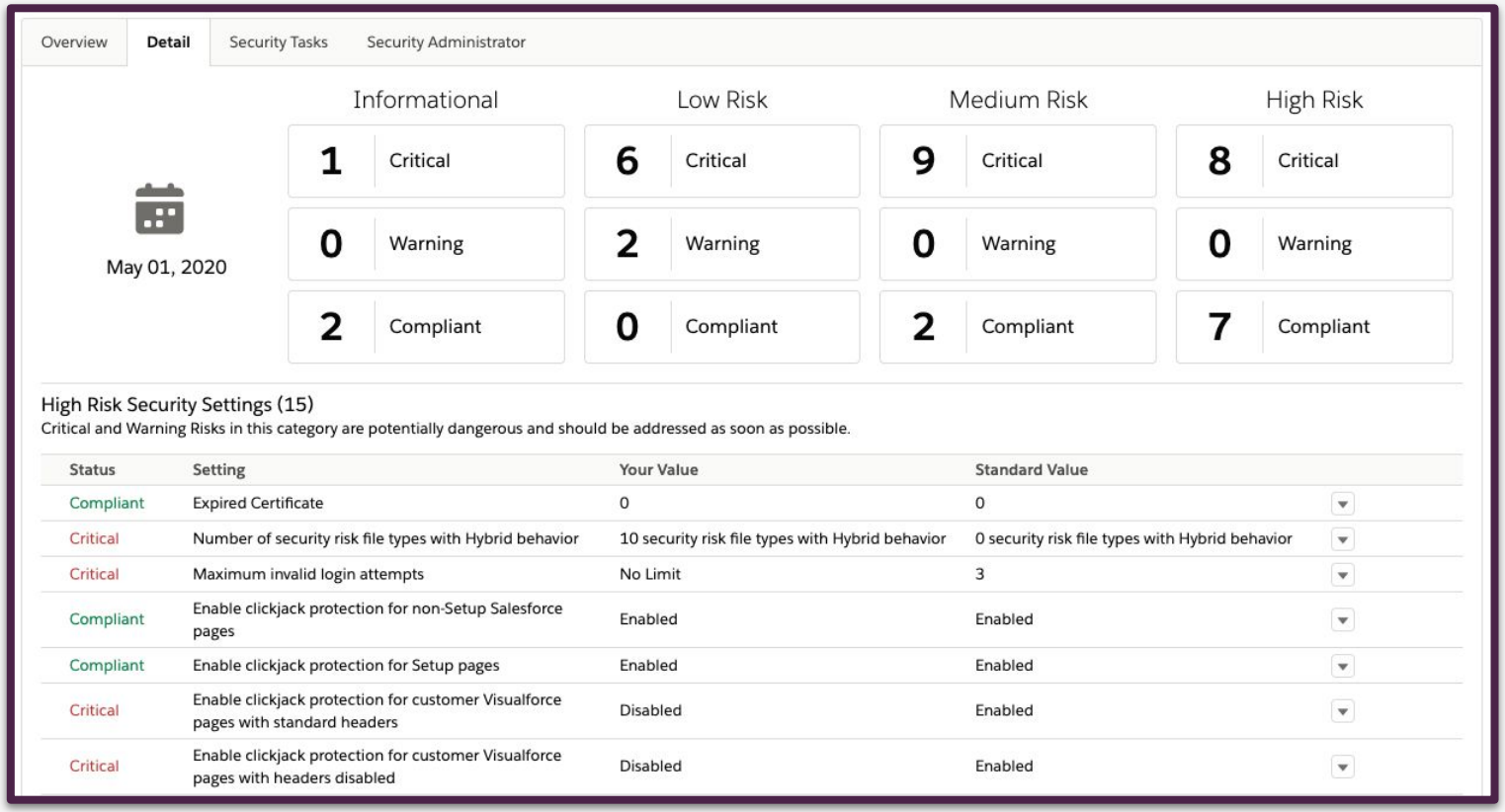
This tab will show you all of your health checks for this org sorted by date, this way you can track security trends and spot changes in the health check.



Navigating Multi-Org Security Summary

Selected Org - Details

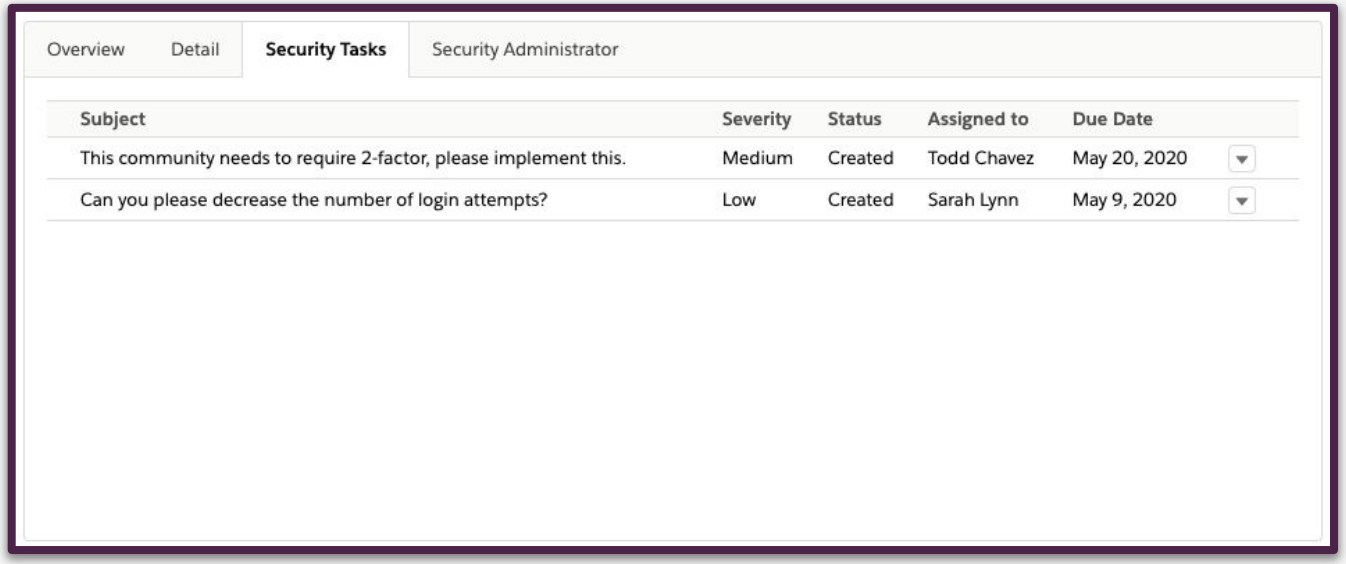
The detail view will give you an indepth look at each days security health check.

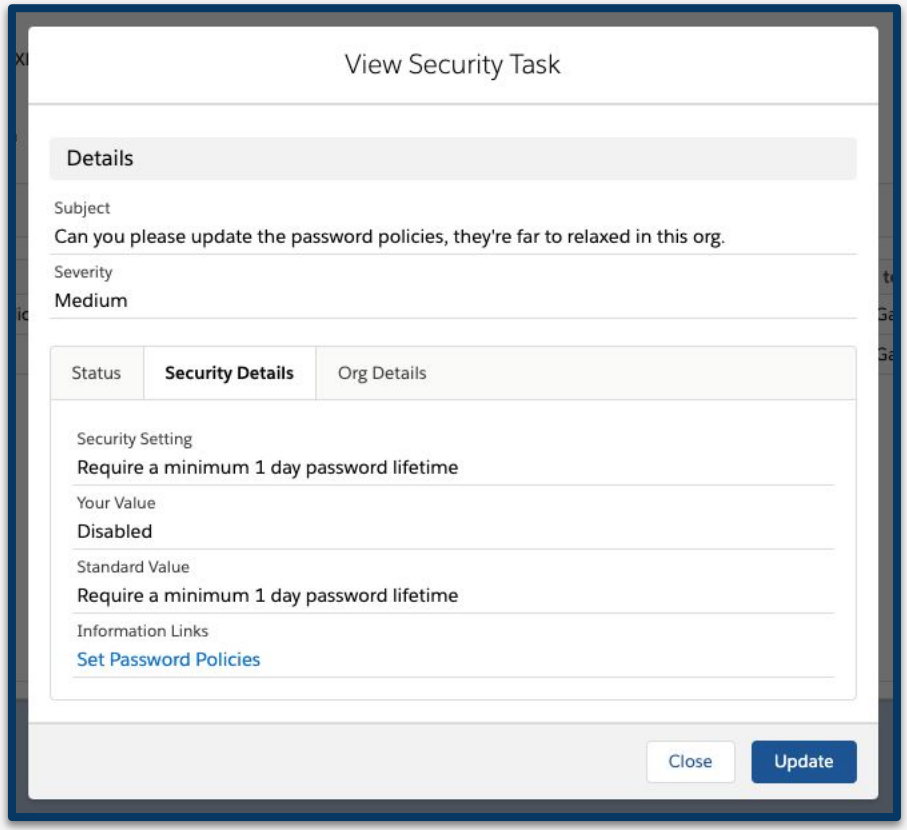


Navigating Multi-Org Security Summary

Selected Org - Security Tasks

The security task detail view gives you a list of all the tasks associated to the selected org.



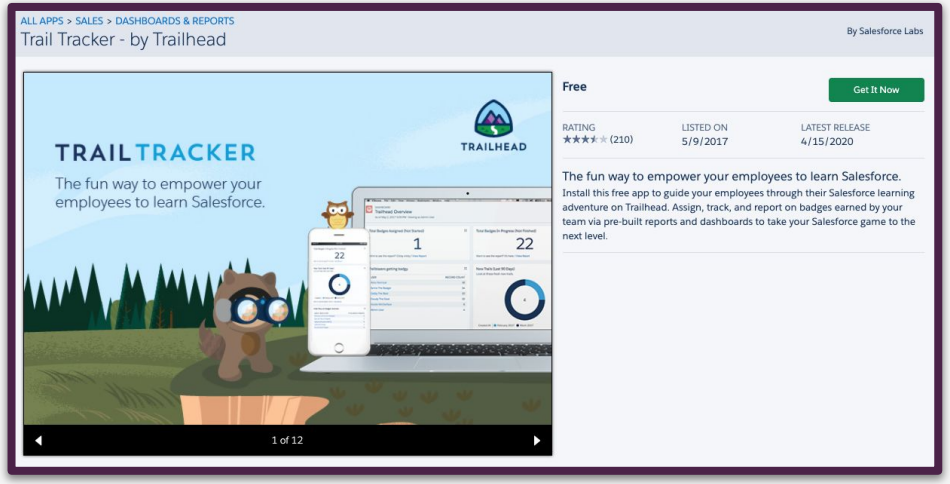


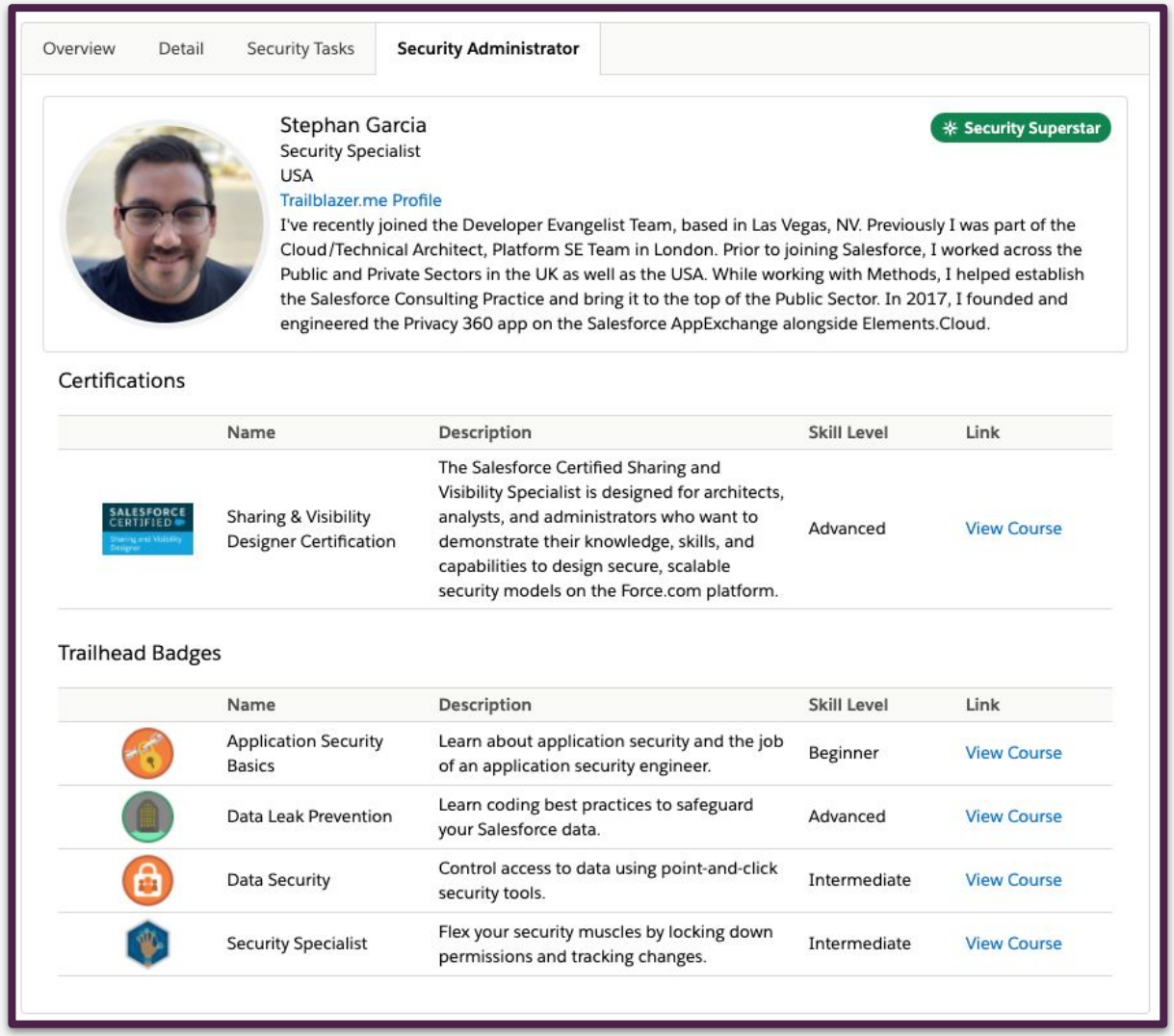
Navigating Multi-Org Security Summary

Selected Org - Security Admin

View the Admin who is in charge of security for the selected org - pull in their user detail from their record and let them show off their security Trailhead badges & certifications.

This functionality could be extended Trail Tracker by Salesforce Labs - available now on the AppExchange!





Troubleshooting

Things to check if it doesn't seem to be working and you followed all the steps....

Authenticated Method (Option 1)

- Does the user you have configured in the child Named Credentials have access to the Connected App? [check Step 11 of the Central configuration]
- Does the url you entered in Child step 8 match the domain of the central org? [check it is ...my.salesforce.com]

Authenticated Method (Option 2)

- Does the url you configured in Central step 14 match the value you entered in Child step 13 ?

Both Methods (Metadata configuration)

- In the Central step 17 or Child step 14 - did you rename the Label **and** the Name? If the Name is left as 'Configuration' it will not sync.
- In the Child configuration - Does the Named Credentials in the cloned metadata record match the name you set in the Named Credentials?
- In the Child configuration - Does the Token in the cloned metadata record match the value generated in the central org Security Health Check Org record?


thank you
BLAZE YOUR TRAIL
salesforce